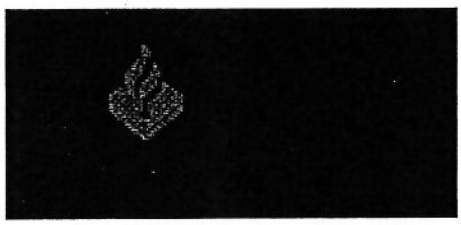
# - Informatiegestuurde Aanpak van Botnets -

## Plan van aanpak

**<<< Vertrouwelijk >>>**

**Wellicht anders dan de meeste proeftuinen binnen het cybercrime versterkingsprogramma, betreft deze proeftuin een daadwerkelijk operationeel onderzoek van de Dienst Nationale Recherche. Vanwege de vertrouwelijkheid van onderzoeken op dit niveau, wordt extra zorgvuldigheid verzocht m.b.t. het beheer en de verspreiding van de inhoud van dit document.**




| | |
|---|---|
| Naam regio: | Korps Landelijke Politiediensten, Dienst Nationale Recherche, Team High Tech Crime |
| Project/proeftuin: | Informatiegestuurde Aanpak van Botnets |
| Thema: | Versterking informatiepositie cybercrime |
| Projectleider: | S. 1 |
| Datum: | 05-06-2009 |
| Versie: | v1.2 |

**Versiebeheer**

| Versie | Datum | Status | Omschrijving | Auteur |
|---|---|---|---|---|
| 0.1 | 10-03-2009 | Opstellen | Eerste opzet | |
| 0.2 | 21-04-2009 | Opstellen | Aanvullen | |
| 0.3 | 23-04-2009 | Aanpassen | o.b.v. feedback S.1 | |
| 0.4 | 29-04-2009 | Aanpassen | o.b.v. feesback S.1 en (lopend, nog niet geheel afgerond), aanpassingen h2, h3 en h4 moeten nog | S.1 |
| 0.5 | 07-05-2009 | Aanpassen | Feedback S.1 en rest va | |
| 0.6 | 12-05-2009 | Aanpassen | Feedback | |
| 0.7 | 13-05-2009 | Aanpassen | Diverse wijzigingen, eigen inzicht | |
| 0.8 | 14-05-2009 | Aanpassen | o.b.v. feedback S.1 en S.1 | S.1 |
| 0.9 | 28-05-2009 | Aanpassen | o.b.v. overleg van 19 mei 2009 | |
| 1.0 | 29-05-2009 | Aanpassen | o.b.v. feedback S.1 | |
| 1.1 | 02-06-2009 | Aanpassen | o.b.v. feedback | |
| 1.2 | 05-06-2009 | Aanpassen | Schoonheidsfoutje in layout aangepast | |

**Distributie**

| Versie | Datum | Van | Aan | Medium |
|---|---|---|---|---|
| 0.2 | 21-04-2009 | | | Email |
| 0.3 | 23-04-2009 | | | Email |
| 0.4 | 21-04-2009 | | | Email |
| 0.6 | 12-05-2009 | | | Email |
| 0.8 | 14-05-2009 | | | Email |
| 0.8 | 25-05-2009 | S.1 | S.1 | Email |
| 1.0 | 28-05-2009 | | | Email |
| 1.1 | 02-06-2009 | | | Email & fysiek |

| | | | | |
|---|---|---|---|---|
| 1.2 | 08-06-2009 | 5.1 | | 5.1 |

**Goedkeuring**

| **Opdrachtgever** | **Opdrachtgever** |
|---|---|
| Organisatie: Korps Landelijke Politiediensten<br>Functie: Korpschef<br>Naam: 5.1 | Organisatie: Landelijk Parket<br>Functie: Hoofdofficier<br>Naam: 5.1 |
| Datum: | Datum: |

| **Opdrachtnemer** | **Opdrachtnemer** |
|---|---|
| Organisatie: Korps Landelijke Politiediensten<br>Dienst Nationale Recherche<br>Team High Tech Crime<br>Functie: Senior Adviseur / Projectleider<br>Naam: 5.1 | Organisatie: Parket<br>Functie: -<br>Naam: - |
| Datum: | Datum: |

**INHOUDSOPGAVE**

## Managementsamenvatting

Een belangrijk onderdeel binnen Cybercrime en High Tech Crime is het gebruik van Botnets. Een Botnet is een netwerk van geïnfecteerde computers, waarbij een deel van de rekencapaciteit en netwerkfunctionaliteit van de geïnfecteerde computers gekaapt wordt en ter beschikking komt te staan van een cybercrimineel. Het vormt de basis voor vervolgstappen binnen cybercrime, zoals het versturen van spam, het uitvoeren van dDOS-aanvallen[1], het middels keylogging stelen van persoonlijke gegevens, het omleiden van internet-bankierverkeer, etc. In het Strategiedocument 2009-2011 is tussen het Landelijk Parket en Team High Tech Crime overeen gekomen dat er binnen de aanpak van cybercrime meer aandacht uit zal gaan naar onder andere:

- de aanpak van Botnets
- versterking van de informatiepositie
- versterking van publiek-private samenwerkingsverbanden
- opwerpen van drempels

In het verlengde van deze uitgangspunten is Team High Tech Crime op zoek gegaan naar een aanpak van Botnets. Hierbij zou het aanbod van Botnet-zaken niet 'toevallig' middels een aangifte of rechtshulpverzoek bij het team terecht komen, maar zou er een dusdanige informatiepositie ten aanzien van Botnets moeten worden opgebouwd dat het team gericht kan kiezen welke Botnets aan te pakken, bijvoorbeeld vanwege de aard en omvang van een specifiek Botnet, alsmede een relatie met Nederlandse verdachten, Nederlandse slachtoffers en/of gebruikte Nederlandse infrastructuren. De aanpak kan vervolgens zowel repressief als preventief zijn. De doelstelling is om beide te doen.



Het KLPD en het OM willen de voorgenomen aanpak aanmelden als proeftuin binnen de Intensiveringsprogramma's Cybercrime van het OM en de Politie. Hierdoor is enerzijds beter geborgd dat de opgedane kennis en ervaring politie-breed en OM-breed uitgeleerd kan worden. Anderzijds biedt dit de mogelijkheid om voor de kosten van bijzondere benodigde resources een beroep te doen op de daarvoor landelijk vrijgemaakte gelden.

Het project levert verschillende producten op. In praktische zin zullen dit zijn:

- Een realtime overzicht en inzicht in een groot aantal wereldwijd actieve Botnets
- Aanhoudingen van verdachten van het opzetten dan wel gebruiken van bepaalde Botnets
- Barrières voor Botnet-activiteiten in Nederland.
- Algemene kennis en ervaring voor de aanpak van Botnets

[1] distributed Denial of Service-aanvallen, een methode waarbij middels een Botnet overbelasting wordt gegenereerd van doelwitcomputers (zoals servers) waardoor deze vastlopen.

Daarnaast zullen er een aantal kennisproducten worden opgeleverd:

- Kennisdocument ten aanzien van vereiste publiek-private samenwerkingsverbanden voor verbetering van de informatiepositie, voor repressieve tactieken en preventieve tactieken ten aanzien van Botnets.
- Kennisdocument over decryptietechnieken bij Botnets
- Kennisdocument ten aan zien van juridische aspecten omtrent de opsporing en vervolging van Botnets.
- Kennisdocument ten aanzien van de ontmanteling van Botnets

Deze kennisdocumenten zullen ter beschikking worden gesteld aan regiokorpsen en BDE's. Tevens zal de inhoud ervan op gerichte momenten gericht aan deze partijen worden uitgeleerd.

Ook zal het project verschillende rapportages opleveren:

- tussentijdse rapportages
- (min. 1) bestuurlijke rapportage
- eindevaluatie

4.1

## Inleiding

U treft hierbij aan een format voor het te maken plan van aanpak. Niet alle vragen kunnen in elk proeftuinvoorstel worden beantwoord, dit is ook afhankelijk van het thema en de concrete strafzaak. In de bijlage wordt nader ingegaan op een aantal aspecten uit de intensiveringsprogramma's, die van belang zijn bij het opmaken van het plan van aanpak.

Het plan van aanpak (met concrete doelstellingen) is een document met een aantal functies:

1. Voor politie/OM: helder krijgen wat er met de proeftuin wordt beoogd: (wat willen we bereiken).
2. Het plan van aanpak is een instrument om inhoudelijk te monitoren (naast de P&C cyclus waarin financiële verantwoording wordt afgelegd over de besteding van het verkregen budget) of de (vooraf bepaalde) doelstellingen in de proeftuinaanpak worden gerealiseerd. Een zo "SMART"mogelijke omschrijving van doelstellingen met tijdpad is aan te raden. Door vooraf de aspecten waarop gemonitord gaat worden vast te leggen, wordt het ook makkelijker om te sturen op de proeftuinaanpak (door de indieners van het voorstel). Door middel van auditatie of visitatie zal de stand van zaken in de proeftuin worden gemonitord. Het plan van aanpak maakt een zelfevaluatie na afloop makkelijker.
3. Formaliseren van het proeftuinvoorstel: Verantwoordelijkheden (voor besteding budget en realisatie doelstellingen) worden benoemd.
4. Alle proeftuinen worden in opdracht van het Parket-Generaal geëvalueerd door wetenschappers (onder regie van het WODC)
5. Een belangrijk onderdeel van het plan van aanpak is, dat wordt aangegeven op welke wijze ervaringen/kennis ter kennis wordt gebracht aan het land (uitleren best practices, barrières in het barrière model, wijze en tijdstip van bestuurlijk rapporteren, ontwikkeling intelligence en informatie producten, nieuwe functies etc.)

# 1. Doelstelling

## 1.1 Aanleiding

- Beschrijf de aanleiding van het project / de proeftuin

Het Kabinet heeft in het kader van haar veiligheidsprogramma "Veiligheid begint bij Voorkomen" voor de bestrijding van financieel-economische criminaliteit, georganiseerde misdaad en cybercrime gelden vrijgemaakt. De politie en het Openbaar Ministerie (OM) hebben zich in dat kader in de visiedocumenten "gezamenlijke landelijke prioriteiten politie 2008-2011" en Visie en Plan van Aanpak Programma Cybercrime elk gecommitteerd aan het leveren van een bijdrage aan het (opstellen en) uitvoeren van de intensiveringsprogramma's die daaruit voortkomen.
Door de Raad van Hoofdcommissarissen (RHC) is met betrekking tot cybercrime het Programma Aanpak Cybercrime (PAC) ontwikkeld. Dit heeft geresulteerd in het "Programmaplan PAC" van 14 februari 2008. Het College van Procureurs-Generaal heeft in januari 2008 het "Intensiveringsprogramma Cybercrime", visie en plan van aanpak Openbaar Ministerie uitgebracht.
In juni 2008 hebben zowel de Board Opsporing van de RHC als het College van Procureurs-Generaal, een brief aan respectievelijk de regiokorpsen en de Hoofdofficieren van Justitie doen uitgaan waarin werd verzocht om samen proeftuinvoorstellen voor de aanpak van 7 benoemde thema's te komen. Een van de thema's binnen de aanpak van cybercrime is 'ICT als doelwit'.
Binnen het hierboven beschreven kader dienen het Landelijk Parket en het Team High Tech Crime (THTC) van de Nationale Recherche van het Korps Landelijke Politiediensten in juni 2009 een proeftuinvoorstel in met betrekking tot de aanpak van cybercrime, meer specifiek de aanpak van het thema 'ICT als doelwit'. De proeftuin ziet op de informatiegestuurde aanpak van Botnets.
Hieronder volgt een korte uiteenzetting van de achtergrond van THTC.

## 1.2 Team High Tech Crime

De aanpak van cybercrime is belangrijk aangezien steeds meer burgers, bedrijven en overheden worden geconfronteerd met deze vorm van criminaliteit, vanwege het toenemende gebruik van internet en de invloed daarvan op de maatschappij. Onder meer bijzondere vormen van cybercrime die kunnen worden gekwalificeerd als vormen van zware en georganiseerde misdaad moeten worden aangepakt. Om deze impuls op landelijk niveau vorm te kunnen geven is per 1 januari 2007 het Team High Tech Crime (THTC) operationeel.[2] Dit team wordt binnen het traject Koers 2010 ingebed in de organisatie als Speciaal Rechercheteam binnen de Dienst Nationale Recherche van het Korps Landelijke Politiediensten. Het team heeft opsporing van bijzondere vormen van cybercrime – vervolgens *high-tech crime* genoemd - als primaire taak. Het THTC werkt daarbij intensief samen met (inter)nationale partners van politie- en justitiële organisaties en in de publieke en private sector.[3]

De doelstelling van het THTC is als volgt geformuleerd[4]:

*Het effectief en efficiënt bestrijden van high-tech crime op nationaal en internationaal niveau, door*

---

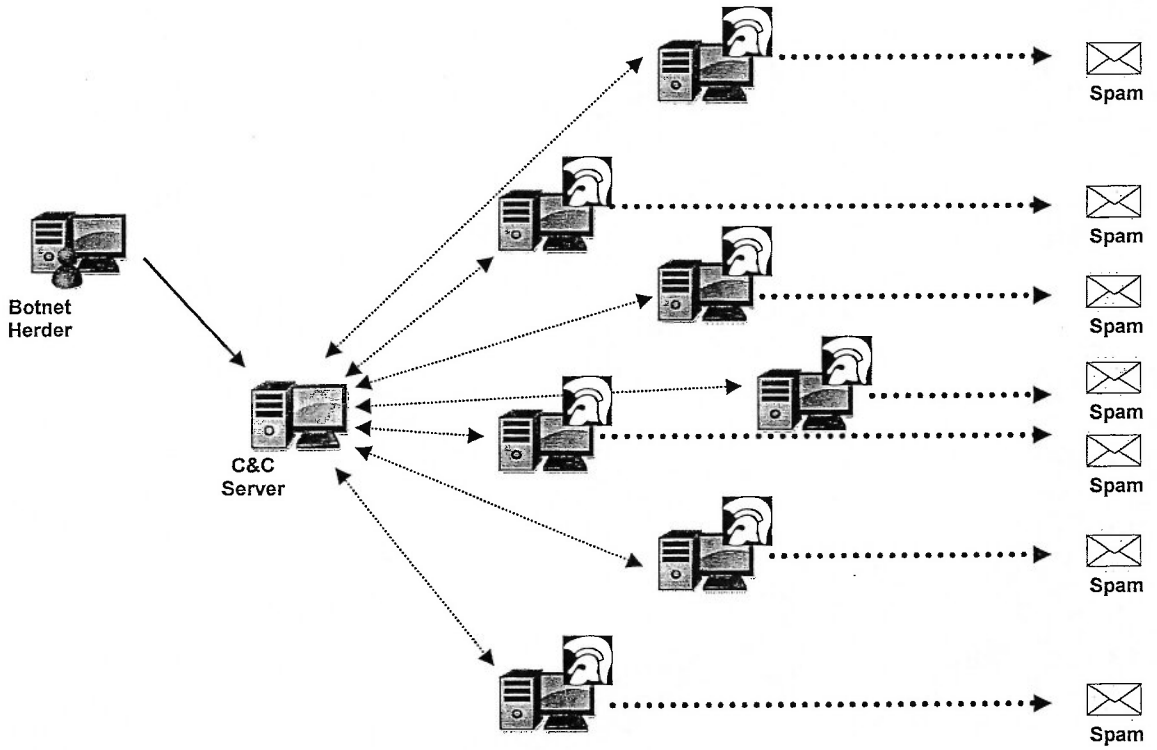
[2] Bedrijfsplan Team High Tech Crime/ DNR/ KLPD. E. Jansen/ H. Bouter/ J. van Oss, 20 november 2006
[3] Aanbieding eindadvies van de projecten NPAC en NHTCC, Brief aan de Voorzitter van de Tweede Kamer der Staten Generaal, 18 mei 2006
[4] Visiedocument Team High Tech Crime 2007-2010, A. Sey/ P. Zinn/ J. van Oss/ M. Schuurbiers

- *het verrichten van opsporingsonderzoeken naar high-tech crime,*
- *het ontwikkelen, verzamelen en delen van informatie, kennis en expertise die nodig is om opsporingsonderzoeken naar high-tech crime succesvol uit te voeren en*
- *de ontwikkeling en toepassing van aanvullende strategieën in het kader van tegenhouden van high-tech crime.*

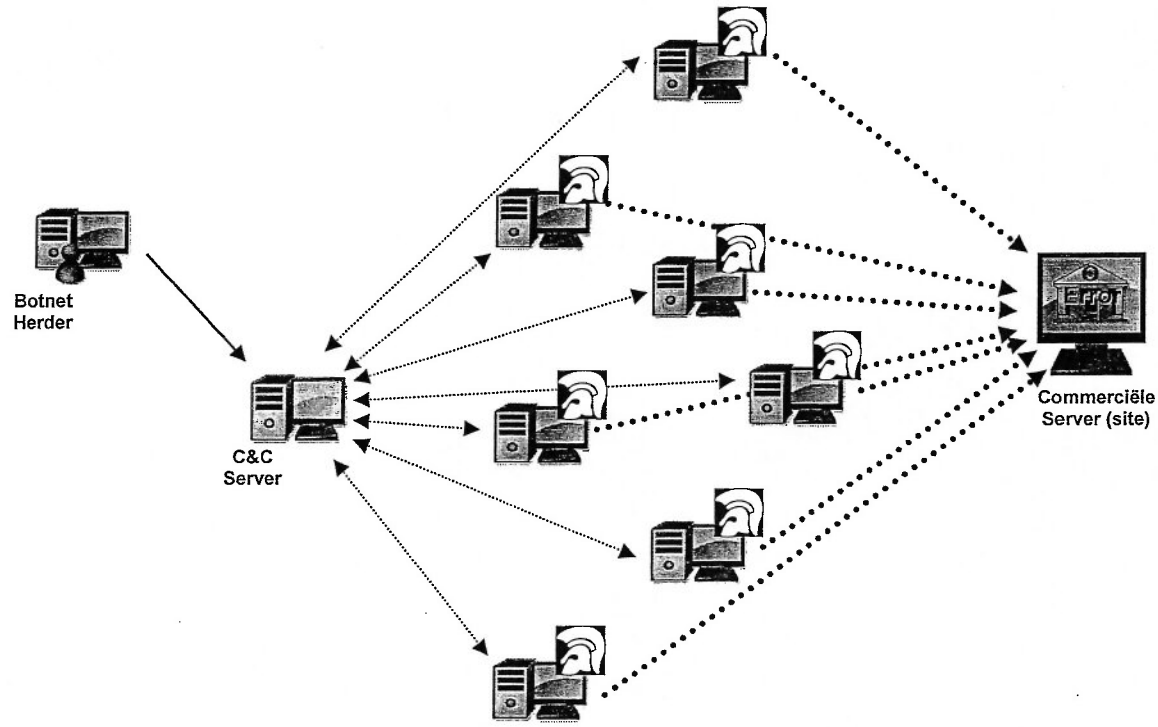
## 1.3 Botnets

Een belangrijk onderdeel binnen Cybercrime en High Tech Crime is het gebruik van Botnets. Een Botnet is een netwerk van geïnfecteerde computers, waarbij een deel van de rekencapaciteit en netwerkfunctionaliteit van de geïnfecteerde computers gekaapt wordt en ter beschikking komt te staan van een cybercrimineel. Van de besmetting merkt de gebruiker doorgaans weinig; dit kan gebeurd zijn door het binnenhalen van een virus per mail, of zelfs na het bezoeken van een besmette webpagina. Ook van het kapen van een deel van zijn computer merkt hij weinig; de gebruiker kan nog gewoon zijn normale bezigheden op zijn computer uitvoeren. Ook is deze kaping verder niet zichtbaar.

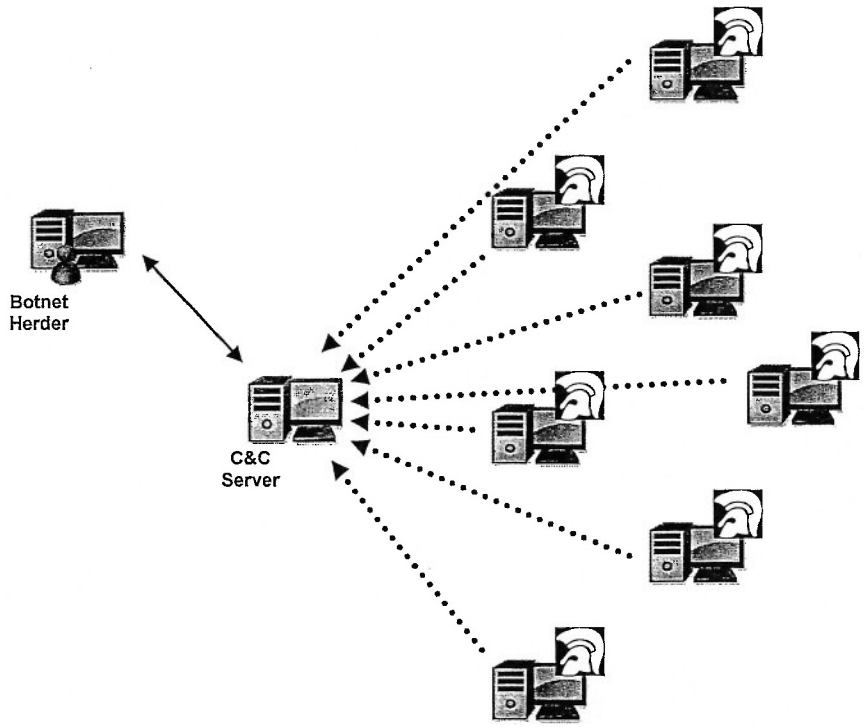
De gebruikte techniek voor zowel de primaire besmetting als de uiteindelijke besturing van Botnets lopen uiteen, feit is echter dat Botnets een krachtig een flexibel hulpmiddel zijn voor cybercriminelen om uiteenlopende strafbare feiten te plegen. Ter illustratie staan in de navolgende figuren enkele illustraties van criminele toepassingen van Botnets die vanuit een centrale Command&Control-server bestuurd worden.




*Figuur 1: Het versturen van Spam. De beheerder van het Botnet (links, de 'herder') geeft via zijn centrale Command&Control-server opdrachten aan individuele bots (midden) om massaal spamberichten te gaan versturen.*




*Figuur 2: Het uitvoeren van een dDOS-aanval. Hierbij geeft de beheerder van het Botnet (links, de 'herder') via zijn centrale Command&Control-server opdrachten aan individuele bots (midden) om massaal contact te zoeken met een server, waardoor deze overbelast raakt.*



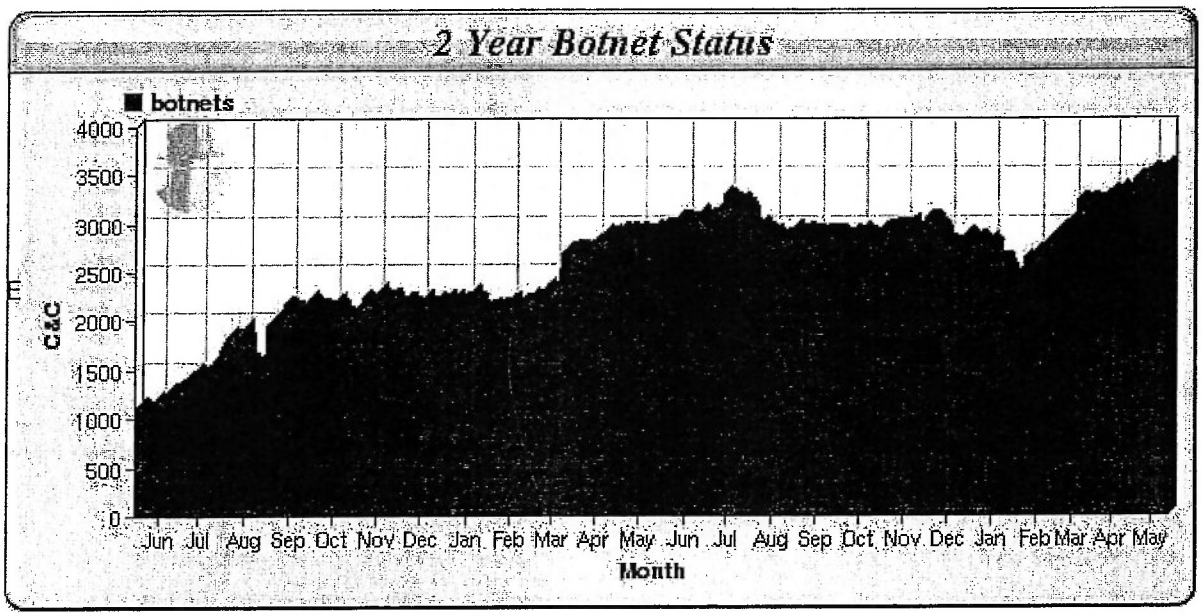

*Figuur 3: Keylogging. Hierbij worden alle toetsaanslagen van individuele bots (rechts) naar een centrale Command&Control-server gestuurd (midden), waar ze ter beschikking komen te staan van de beheerder van het Botnet (links, de 'herder').*

Omdat Botnets zo'n belangrijke basisfunctionaliteit vervullen binnen verschillende vormen van cybercrime, is het van belang om er onder andere binnen de opsporing prominente aandacht aan te besteden. Ook binnen de speerpunten is dit fenomeen benoemd. Het Landelijk Parket en Team High Tech Crime hebben in het Strategiedocument de volgende speerpunten gedefinieerd voor de periode 2008-2011[5]:

- De aanpak van **Botnets** als belangrijkste technisch hulpmiddel voor het uitvoeren van uiteenlopende criminele activiteiten
- Het versterken van de **informatiepositie** met als doel een beter zicht op criminele organisaties en hun werkwijzen, en een instrument om keuzes te kunnen maken in aan te pakken zaken. Middelen ter versterking van de informatiepositie zijn onder andere samenwerking met private partijen, aanboren van nieuwe bronnen, nauw contact met buitenlandse politie en justitie, nodale informatiewinning en versterking van de CIE.
- Versterking van de **publiek-private samenwerking** met als doelen versterking van de informatiepositie, verdeling van de capaciteitsdruk, bescherming van de vitale infrastructuur en in het kader van de doelstelling tegenhouden het gezamenlijk **opwerpen van drempels** voor High Tech Criminelen. In het kader van tegenhouden maken THTC en het LP zich sterk voor de oprichting van een Joint Taskforce van politie, banken en internetproviders.
- Verdere **ontwikkeling kennis en expertise**, met als doel adequater te kunnen reageren en uiteindelijk zelfs proactief te kunnen zijn in de continue veranderende High Tech Crime wereld. Onder deze noemer valt het verder uitbouwen van het THTC en LP-netwerk van partners en relevante partijen, alsmede het verhogen van het kennisniveau van de medewerkers met als doel samen met de betreffende partners adequater te kunnen reageren.
- **Innovatief rechercheren** – enerzijds omdat High Tech Crime zaken zonder innovatief rechercheren vaak eenvoudigweg niet op te lossen zijn, anderzijds om voldoende jurisprudentie te genereren om zinvolle bijstellingen van de Wet Computercriminaliteit mogelijk te maken. Daarnaast dienen dergelijke concrete opsporingsonderzoeken de basis te vormen voor kennis en expertise die een verscheidenheid aan preventieve adviezen mogelijk maakt.

Wanneer we dit totaaloverzicht van speerpunten verder bekijken, is duidelijk dat onder andere de informatiepositie een belangrijke plaats krijgt toebedeeld. Dit geldt zeker ook voor de aanpak van Botnets. Een onafhankelijke bron geeft aan dat er in 2008 gemiddeld ongeveer 2500 verschillende Botnets bekend waren, welke tot 4 december 2008 gezamenlijk verantwoordelijk waren voor ruim 193.000 dDos aanvallen, gericht op ongeveer 20.000 verschillende doelen[6]. Inmiddels is dit aantal gestegen tot ongeveer 3500. Een andere bron geeft aan dat over het eerste kwartaal van 2009 bijna 12 miljoen IP-adressen zijn gedetecteerd die dienst doen als zombie[7] (= stijging van 50% tov 1e kwartaal 2008).[8]

[5] Strategiedocument High Tech Crime – LP & KLPD
[6] Bron: Shadowserver Foundation, 4 december 2008, http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts
[7] De term 'zombie' wordt gebruikt als aanduiding voor een geïnfecteerde computer die daardoor deel uitmaakt van een Botnet. Eem Zomie wordt ook wel een bot genoemd.
[8] Bron: McAfee Dreigingsrapport I 2009, p4.




*Figuur 4: Overzicht van geregistreerde Botnets door de Shadowserver Foundation, mei 2009*

Het zal onmogelijk zijn om alle wereldwijd actieve Botnets aan te pakken. Het is daarom belangrijk om eerst te bekijken welke Botnets er daadwerkelijk zijn, van waaruit ze bestuurd worden en/of voor welke doelen ze gebruikt worden. Op deze manier zouden vervolgens de juiste anticiperende keuzes gemaakt kunnen worden. Hierbij kan gekozen worden voor bijvoorbeeld gerichte opsporingsonderzoeken op specifieke Botnets, bijvoorbeeld Botnets met Nederlandse beheerders of Botnets met Nederlandse slachtoffers. Echter kan de informatiepositie ook dienen voor barrièrestrategieën, bijvoorbeeld door Nederlandse (en/of buitenlandse) Command&Control-servers uit de lucht te halen of de controle over dergelijke servers over te nemen en de Botnets daarmee van binnenuit te ontmantelen.

## 1.4 Probleemstelling

- Geef een beschrijving van de geconstateerde problematiek (landelijk/regionaal) waar de proeftuin op aansluit (probleemstelling) ook in relatie tot de maatschappelijke relevantie

Zoals in de vorige paragraaf reeds is beschreven staan Botnets aan de basis van verschillende vormen van criminaliteit. Met toenemende regelmaat lijkt de kern van een Botnet te bestaan uit modulaire programmatuur. Via een bot wordt additionele software op de geïnfecteerde computer gedownload en geïnstalleerd. Dat kunnen emailers zijn (om spam te versturen), maar ook keyloggers (om toetsaanslagen vast te leggen). Met keylogging kunnen eveneens identiteitsgegevens worden gestolen, alsmede bijvoorbeeld creditcardgegevens, die vervolgens voor tal van zaken worden misbruikt of worden doorverhandeld.

Daarnaast kunnen met dDos-aanvallen[9] vernielingen worden aangericht vanuit ideologische motieven (bijvoorbeeld overheidssites platleggen), maar er kunnen bijvoorbeeld ook bedrijven mee worden afgeperst door te dreigen met het offline halen van een website of netwerk. Ook worden Botnets tegenwoordig gebruikt voor het gestructureerd (op afroep) omleiden van internet-

[9] distributed Denial of Service-aanvallen, een methode waarbij middels een Botnet overbelasting wordt gegenereerd van doelwitcomputers (zoals servers) waardoor deze vastlopen.

bankierverkeer, of als verduisteringswegen om zo min mogelijk eigen sporen achter te laten bij op afstand inbreken op computers[10]. Al met al vormen Botnets dus een basis voor uiteenlopende vormen van cybercrime, waar met name door de omvang op grote schaal burgers slachtoffer van kunnen worden. Botnets worden dan ook niet voor niets door alle vooraanstaande partijen vanuit zowel de publieke als private sector beschouwd als belangrijk aandachtspunt voor de bestrijding van cybercrime.

## 1.5 De proeftuin

- Geef een korte beschrijving van de inhoud van de proeftuin en (de relatie tot) het thema
- Geef aan welke casuïstiek in de proeftuin wordt ingebracht (zonder operationele informatie)

De proeftuin zal erop gericht zijn om Botnets en daarmee gepaard gaande effecten te bestrijden. Aangezien Botnets per definitie grensoverschrijdend zijn, bestaat er op voorhand een risico dat een aanpak door middel van gerichte opsporing, vervolging en/of verstoring verzandt in items op wereldschaal die Team High Tech Crime niet altijd (alleen) op kan lossen. Om dit risico te verkleinen zal er met betrekking tot de bestrijding getracht worden steeds zoveel mogelijk relatie te zoeken met de volgende items:

- Botnets met *Nederlandse verdachten* of verdachten die vanuit Nederland werken
- Botnets met *Nederlandse slachtoffers* (personen danwel instellingen of bedrijven)
- Botnets waarbij *Nederlandse infrastructuren* als fundamenteel onderdeel worden gebruikt

3.1 / 4.1

3.1 / 4.1

## 1.6 De vernieuwende en/of onderscheidende elementen

- Geef een korte beschrijving van het onderscheidend vermogen van de proeftuin (bijvoorbeeld wijze van werken, benodigde expertise of het gebruik van intelligence)
- Geef kort aan of sprake is van een programmatische aanpak en/of een innovatief strafrechtelijk onderzoek
- Geef een korte beschrijving van de (kansrijke) omgeving waarbinnen de proeftuin wordt gedraaid (bijvoorbeeld experimenteel op het gebied van samenwerking of door het inzetten van nieuwe vormen van kennis)

Nb Een verdere uitwerking hiervan komt in hoofdstuk 2 Aanpak en planning

*Operationele componenten*

3.1 / 4.1

*Juridische componenten*

Strafrechtelijk gezien kent de methodiek ook diverse innovatieve aspecten. Een van de vragen die bijvoorbeeld aan de orde komt is welke strafvorderlijke bevoegdheden er nodig zijn voor de inzet van de bovengenoemde tool. Betreft het hier bijvoorbeeld een vorm van observatie, stelselmatige informatie-inwinning of infiltratie? Is sprake van het monitoren van communicatie of juist van gedrag of andere handelingen?, Een tweede vraag die zich aandient is die van de grondslag van een opsporingsonderzoek: Titel VIa of Titel V.

Ten derde dient zich de juridische vraag aan of bij het 'overnemen' van een Botnet (via de C&C server) sprake is van handelen dat een bijzondere grondslag behoeft of dat dit valt onder de algemene taakstelling van art. 2 Politiewet.

Tot slot speelt de vraag van de mogelijkheden tot opsporing op afstand in geautomatiseerde werken die zich in het buitenland bevinden. Het uitwerken van de juiste juridische basis van de genoemde aanpak van Botnets, maakt daarom ook deel uit van de proeftuin.

3.1 / 4.1

## 1.7 Doelstelling proeftuin

- Geef aan wat de doelstelling van de proeftuin is en waaraan het een bijdrage levert
- Geef concreet (SMART = Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden) aan welk(e) doelstelling(en) in de proeftuin worden beoogd
- Geef aan hoe de vernieuwende en/of onderscheidende elementen in de proeftuin tot uitdrukking komen en een bijdrage leveren aan de doelstelling

De doelstellingen van deze proeftuin luiden als volgt (op volgorde van prioriteit):

1. Betere informatiepositie t.a.v. Botnets
   a. *Specifiek*:

3.1 / 4.1

   b. *Meetbaar*: het observeren van de Botnet-activiteit moet realtime geschieden. De doelstelling is om van minimaal 750 verschillende Botnets hun activiteiten te kunnen observeren. Daarbij moeten alle commando's gelogd worden. De hoeveelheid daarvan kan sterk uiteenlopen per Botnet.
   c. *Acceptabel*: de aanpak past binnen het beleid van Team High Tech Crime voor 2009-2011, namelijk verbetering van de informatiepositie en de aanpak van Botnets.

d. *Realistisch*:

e. *Tijdgebonden*: 31/4.1/61

f. *Vernieuwende elementen*:

2. Gericht repressief opsporingsonderzoek naar het gebruik van bepaalde Botnets
   a. *Specifiek*: dit onderzoek zal plaatsvinden bij die Botnets die op basis van de beschikbare informatie blijkbaar gericht zijn tegen Nederlandse bedrijven en/of bestuurd worden door Nederlandse verdachten en/of waarbij gebruik wordt gemaakt van Nederlandse infrastructuren. Aanvullend kan de potentiële of reeds toegebrechte schade een rol spelen bij de keuze welk Botnet aan te pakken. Deze acties zullen dus volgen nadat een voldoende informatiepositie ten aanzien van de Botnets is bereikt.
   b. *Meetbaar*: dergelijk strafrechtelijk onderzoek zal uiteindelijk moeten leiden tot de aanhouding van 1 of meer verdachten per Botnet.[11]
   c. *Acceptabel:* de aanpak past binnen het beleid van Team High Tech Crime voor 2009-2011, namelijk verbetering van de informatiepositie en de aanpak van Botnets.
   d. *Realistisch*: THTC heeft voldoende know-how, expertise en middelen om op basis van een goede informatiepositie verdachten op te sporen, aan te houden en te verhoren. Ondanks gerichte voorselectie, bestaat er evenwel een gerede kans dat tijdens de opsporing zal blijken dat een verdachte niet te identificeren is, of dat deze zich niet in Nederland bevindt. Echter, ook wanneer er Nederlandse slachtoffers zijn of wanneer Nederlandse infrastructuren worden gebruikt, heeft de aanpak voor THTC prioriteit. Opvolging zal dan gezocht worden in mogelijke uitlevering, dan wel vervolging in eigen land.
   e. *Tijdgebonden*: onderzoekstijd voor het vinden van verdachten kan uiteenlopen, maar zou in principe per geval niet langer dan 3 maanden moeten duren.
   f. *Vernieuwende elementen:* er hebben zich relatief nog weinig verdachten voor de rechter moeten verantwoorden voor het gebruik van Botnets. Het gebruik kan daarnaast uiteenlopend zijn. Het is interessant te bekijken hoe de rechter tegen verschillende vormen van dit computermisbruik aan kijkt.

[11] Bij de beslissing tot gerichte opsporing en vervolging zal de waarschijnlijkheid dat Nederlandse verdachten kunnen worden aangehouden een rol spelen. Denkbaar is evenwel dat opsporing leidt tot de aanhouding van verdachten in het buitenland. Deze omstandigheid kan van invloed zijn op de meetbaarheid van de beoogde resultaten.

3. Preventieve maatregelen t.a.v. de geobserveerde Botnets
   a. *Specifiek*:

31/4.1/6.1

   b. *Meetbaar*:

   c. *Acceptabel*: vanwege de complexiteit van defensiemechanismen bestaat de kans dat een cybercrimineel met behulp van tegenmaatregelen een Botnet waartegen preventieve maatregelen worden genomen, deze alsnog terug onder zijn controle kan brengen. Een dergelijke tegenmaatregel is bijvoorbeeld voorgevallen in onderzoek Lievens.
   d. *Realistisch*: THTC heeft, tezamen met TDE, voldoende know-how en expertise om preventieve maatregelen te bedenken en uit te voeren.
   e. *Tijdgebonden*: de gevolgen van preventieve maatregelen zouden in principe binnen enkele dagen zichtbaar moeten zijn.
   f. *Vernieuwende elementen*: interventiestrategieën van Botnets, bijvoorbeeld door Botnets eigen commando's te geven, is zowel vanuit technisch als juridisch oogpunt uiterst vernieuwend.

Ten aanzien van de toepassing van de nodige bevoegdheden om bovenstaande doelen te bereiken, draagt het Landelijk Parket zorg voor een uitwerking van het juiste juridische kader, de noodzakelijke rechterlijke machtigingen, etc.

## 1.8 Beoogd resultaat

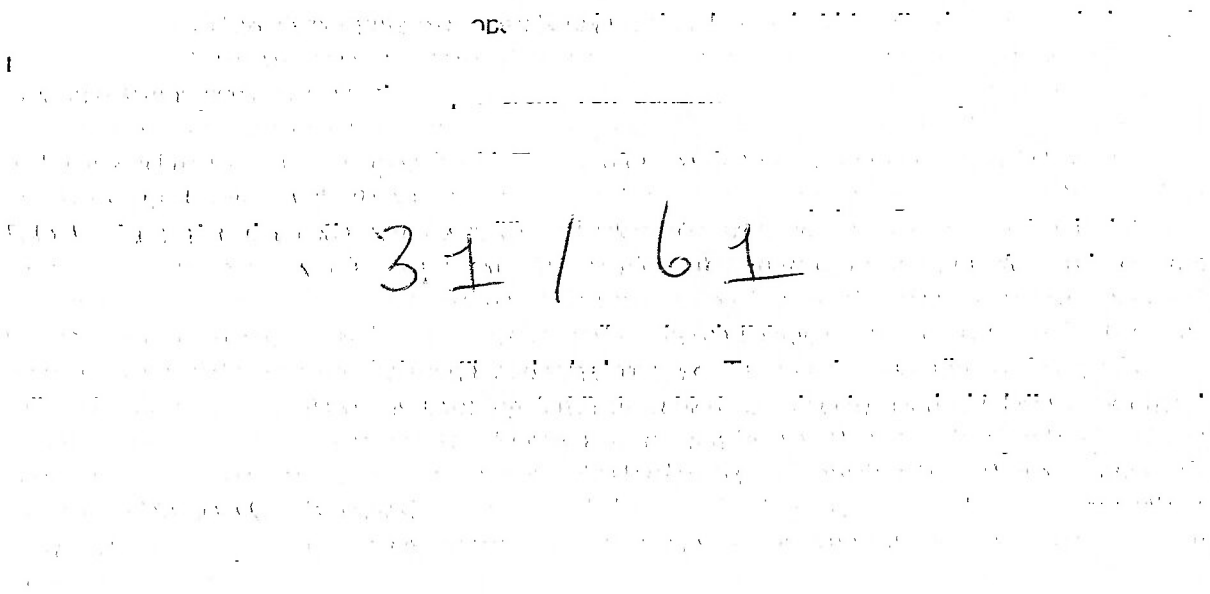
- Geef aan wat het gewenste resultaat is, formuleer dit - indien mogelijk - in concrete producten
- Besteed daarbij in ieder geval aandacht aan het barrièremodel en de bestuurlijke rapportage
- Geef de looptijd van de proeftuin aan

Het primair beoogde resultaat is een betere informatiepositie ten aanzien van Botnets en hun activiteiten. Het zal onmogelijk zijn om alle wereldwijd actieve Botnets hierin te betrekken. Echter, wanneer zicht wordt gekregen op de activiteiten van 750 verschillende Botnets (= ongeveer 25% van alle wereldwijde Botnets) kan dit als succesvol resultaat worden aangemerkt. Deze doelstelling kan verder worden geoptimaliseerd indien op internationaal niveau een structurele informatiedeling kan worden gerealiseerd.

[12] Het ontmantelen van een Botnet kan een zelfstandig spoor vormen binnen het onderzoek, naast het gericht opsporen en vervolgen van personen achter een of meerdere (grotere of gevaarlijker) Botnets.

Het secundair beoogde resultaat is gericht opsporingsonderzoek naar het gebruik van bepaalde Botnets. Hoeveel en welke Botnets dit zijn hangt af van nadere analyse ervan, maar wanneer er naar 3 specifieke Botnets diepgaander opsporingsonderzoek wordt verricht dat leidt tot de identificatie van minimaal 1 verdachte per Botnet, kan dit als succesvol worden aangemerkt. Het succes houdt niet per definitie de aanhouding van een Nederlandse verdachte in. Overdracht van de vervolging naar een ander land behoort ook tot de mogelijkheden.

Het tertiair boogde resultaat zijn preventieve maatregelen t.a.v. geobserveerde Botnets. Wanneer 80% van de bij ons bekende in Nederland gehoste command&control-servers uit de lucht kan worden gehaald, kan dit als succesvol worden aangemerkt. Na afloop van het project kunnen natuurlijk weer nieuwe Nederlandse C&C-servers opduiken. Bij de evaluatie zal besproken worden hoe hiermee om te gaan, bijvoorbeeld continuering van de monitoring, etc.




In totaal kent deze proeftuin, inclusief de doorontwikkeling van de software, een geplande looptijd van naar verwachting 12 maanden.

## 1.9 Omgeving en raakvlakken

- Geef een beschrijving van de maatschappelijke/bestuurlijke context
- Geef een beschrijving van de betrokken partijen en organisaties (lokaal, nationaal, internationaal) en hun rol bij het uitvoeren van de proeftuin (stakeholders)
- Geef dit indien mogelijk weer in een schema/organogram
- Stel de raakvlakken met andere proeftuinen en/of projecten uit de Intensiveringsprogramma's vast

Zoals reeds eerder is aangegeven worden Botnets gebruikt als basismiddel om verschillende vormen van criminaliteit te plegen. Zowel commerciële- als overheidssites worden middels dDos-aanvallen uit de lucht gehaald, en middels keylogging worden identiteitsgegevens en creditcardnummers afgevangen. Ook internetbankierverkeer kan middels Botnets worden omgeleid. Door deze vorm van criminaliteit neemt het vertrouwen in het elektronische (handels)verkeer af. Aangezien dit de laatste

jaren een enorme vlucht heeft genomen en de verwachting is dat dit niet zal veranderen, is het essentieel om de inbreuken in dat vertrouwen zo beperkt mogelijk te laten zijn. Alles bij elkaar brengt dit de Nederlandse samenleving economische schade toe, al is deze op dit moment nog niet in concrete cijfers uit te drukken.
Botnets hebben zoals gezegd een internationaal bereik, en bewustzijn binnen deze internationale omgeving zal een belangrijke rol spelen. Hierbij zal THTC dankbaar gebruik maken van haar inmiddels wijds verspreide netwerk

6.1

Hoewel Botnets weliswaar doorgaans een internationaal bereik hebben, zijn er inmiddels signalen dat Botnets ook binnenlands of zelfs regionaal worden ingezet als middel (bijvoorbeeld dDOS). Uitlering van kennis van dit fenomeen en de aanpak ervan lijkt dan nuttig. Naar verwachting zal de proeftuin hier ook inzichten in verschaffen.

6.1

## 1.10 Afbakening

- Geef hier aan wat de reikwijdte is van de proeftuin. D.w.z. welke resultaten niet binnen het bereik van de proeftuin liggen of kunnen liggen
- Geef aan welke eventuele eisen en randvoorwaarden aan de opdracht gesteld worden door de opdrachtnemer of opdrachtgever

Botnets trekken zich per definitie niets aan van landsgrenzen. Ondanks wellicht goedbedoelde preventieve maatregelen ten aanzien van bepaalde Botnets, bestaat de kans dat bepaalde Botnets desalniettemin zullen blijven voortbestaan via een besturing buiten Nederland om. Deze vallen echter niet binnen het bereik van de proeftuin. Voor de helderheid is het daarom belangrijk om te vermelden dat, ondanks de internationale reikwijdte van Botnets, de nadruk zal liggen op het Nederlandse belang, en wel met de volgende focus:

- Botnets met *Nederlandse verdachten* of verdachten die vanuit Nederland werken
- Botnets met *Nederlandse slachtoffers* (personen danwel instellingen of bedrijven)
- Botnets waarbij *Nederlandse infrastructuren* als fundamenteel onderdeel worden gebruikt

Daarnaast moet worden vermeld dat het onderzoek experimenteel van aard is. Hierdoor zijn niet alle consequenties en onderzoeksrichtingen op voorhand in te schatten. De opdrachtnemers eisen flexibiliteit ten aanzien van bepaalde vooraf gekozen richtingen; er moet genoeg ruimte blijven bestaan om te kunnen anticiperen op voortschrijdend inzicht, uiteraard in overleg met het Landelijk Parket en waar nodig met rechterlijke machtiging.

Verder zal een deel van de te plegen interventies ten aanzien van Botnets waarschijnlijk door private partijen dienen te geschieden. Voorop zal staan een intensieve informatiedeling, waarbij steeds (op convenantbasis en/of vanuit de informele invloedsfeer) zal worden aangedrongen op dergelijke interventies. Het plegen van die interventies is mogelijk echter niet in alle gevallen afdwingbaar, hetgeen van invloed kan zijn op het gewenste eindresultaat. Tekortkomingen daarbij kunnen natuurlijk wel als zinvolle input dienen voor bestuurlijke advisering achteraf.

# 2. Aanpak en planning

## 2.1 Programmatische aanpak en/of innovatieve werkwijze

- Geef een korte (globale) beschrijving van de voorgestane programmatische aanpak en/of de innovatieve werkwijze (strafrechtelijk, bestuurlijk, privaatrechtelijk, publiek-privaat, preventief, internationaal)
- Geef aan op welke wijze de partners worden betrokken in de programmatische aanpak

Nb De concrete invulling en uitwerking van de programmatische aanpak en/of innovatieve werkwijze zal gedurende het project ontstaan, daarom volstaat op deze plaats een (globale) eerste indicatie

De proeftuin is erop gericht om Botnets en daarmee gepaard gaande effecten te bestrijden. Hiervoor zal aan aanpak in eerste instantie gericht zijn op het verbeteren van de *informatiepositie* ten aanzien van Botnets. Als het overzicht er eenmaal is, zal vervolgens primair *strafrechtelijk onderzoek* plaatsvinden naar een aantal specifieke Botnets. Daarna zullen er *preventieve maatregelen* worden genomen om het aantal actieve Botnets te bestrijden. Er zal met betrekking tot de bestrijding getracht worden steeds zoveel mogelijk relatie te zoeken met de volgende items:

- Botnets met *Nederlandse verdachten* of verdachten die vanuit Nederland werken
- Botnets met *Nederlandse slachtoffers* (personen danwel instellingen of bedrijven)
- Botnets waarbij *Nederlandse infrastructuren* als fundamenteel onderdeel worden gebruikt

Daarnaast zullen binnen de proeftuin verschillende kennisproducten worden opgeleverd, die kunnen bijdragen aan het uitleren van de opgedane ervaring, bijdrage aan het Nationaal Dreigingsbeeld en ontwikkeling van bijvoorbeeld nieuwe wetgeving.

Binnen de proeftuin zullen de in de reeds door THTC verrichte onderzoeken, ervaringen en ontwikkelde technieken worden betrokken, aangezien THTC reeds eerder Botnet-gerelateerde onderzoeken heeft gedraaid. Daarnaast zal binnen de proeftuin zoveel mogelijk de publiek-private samenwerking wordt gezocht, en zal ook via zo kort mogelijke lijnen getracht worden samen te werken met buitenlandse opsporingsautoriteiten. Ten aanzien van de publiek-private samenwerking zal onder andere worden samengewerkt met

- Internet Service Providers (voor bijvoorbeeld Notice and Takedown van Command&Control-servers)
- Anti-Virusbedrijven (voor bijvoorbeeld de analyse van bepaalde malware, en voor de benodigde input van Botnet-data in het algemeen.
- Banken (voor bijvoorbeeld het delen van informatie omtrent verdachte IP-adressen, om zo aanvallen op internet-bankierverkeer te voorkomen
- 31/4.1/6.1

31/4.1

3.1/4.1

Het primair beoogde resultaat is een betere informatiepositie ten aanzien van Botnets en hun activiteiten. Het zal onmogelijk zijn om alle wereldwijd actieve Botnets hierin te betrekken. Echter, wanneer zicht wordt gekregen op de activiteiten van 750 verschillende Botnets (= ongeveer 25% van alle wereldwijde Botnets) kan dit als succesvol resultaat worden aangemerkt. Deze doelstelling kan verder worden geoptimaliseerd indien op internationaal niveau een structurele informatiedeling kan worden gerealiseerd.

Het secundair beoogde resultaat is gericht opsporingsonderzoek naar het gebruik van bepaalde Botnets. Hoeveel en welke Botnets dit zijn hangt af van nadere analyse ervan, maar wanneer er naar 3 specifieke Botnets diepgaander opsporingsonderzoek wordt verricht dat leidt tot de identificatie van minimaal 1 verdachte per Botnet, kan dit als succesvol worden aangemerkt. Het succes houdt niet per definitie de aanhouding van een Nederlandse verdachte in. Overdracht van de vervolging naar een ander land behoort ook tot de mogelijkheden.

Het tertiair boogde resultaat zijn preventieve maatregelen t.a.v. geobserveerde Botnets. Wanneer 80% van de bij ons bekende in Nederland gehoste command&control-servers uit de lucht kan worden gehaald, kan dit als succesvol worden aangemerkt. Na afloop van het project kunnen natuurlijk weer nieuwe Nederlandse C&C-servers opduiken. Bij de evaluatie zal besproken worden hoe hiermee om te gaan, bijvoorbeeld continuering van de monitoring, etc.

## 2.2 Instrumenten en barrières

- Geef een globale beschrijving van de toe te passen instrumenten (bijvoorbeeld andere type kennis of nieuwe manieren van werken) en op te werpen barrières die in de proeftuin worden ontwikkeld of uitgeprobeerd

Nb De concrete invulling en uitwerking van instrumenten en barrières zal gedurende het project ontstaan, daarom volstaat op deze plaats een (globale) eerste indicatie

Voor het bereiken van de doelstellingen wordt het ontwikkelde programma 4.1 als basisuitgangspunt genomen. Dit programma is in opdracht van de Duitse overheid speciaal voor Law-Enforcement doeleinden ontwikkeld, en werkt globaal als volgt.

4.1/6.1

4.1/6.1

Er kan echter ook voor gekozen worden om preventieve maatregelen te nemen, bijvoorbeeld door het opwerpen van barrières. Een voorbeeld daarvan is de Botnets van binnenuit te ontmantelen. Dit zou bijvoorbeeld kunnen door alle bekende Command&controlservers via een Notice & Takedownprocedure offline te halen, desnoods zelfs wereldwijd.

3.1/4.1

3.1 / 4.1

## 2.3 Producten

- Geef aan welke producten het resultaat zijn van het project
- Geef aan wanneer de producten worden opgeleverd
- Geef een korte omschrijving van / uitleg over de op te leveren producten

Nb Minimaal worden de volgende producten gevraagd:
- eindevaluatie
- bestuurlijke rapportage
- overzicht van best practices
- tussentijdse rapportages
- (indien mogelijk) toe te passen of beproefde belemmeringen in het barrièremodel
- rapportage aan Taskforce

Het project levert verschillende producten op. In praktische zin zullen dit zijn:
- Een realtime overzicht en inzicht in een groot aantal wereldwijd actieve Botnets
- Aanhoudingen van verdachten van het opzetten dan wel gebruiken van bepaalde Botnets
- Barrières voor Botnet-activiteiten in Nederland
- Algemene kennis en ervaring voor de aanpak van Botnets

Daarnaast zullen er een aantal kennisproducten worden opgeleverd:
- Kennisdocument ten aanzien van vereiste publiek-private samenwerkingsverbanden voor verbetering van de informatiepositie, voor repressieve tactieken en preventieve tactieken ten aanzien van Botnets
- Kennisdocument over decryptietechnieken bij Botnets
- Kennisdocument ten aan zien van juridische aspecten omtrent de opsporing en vervolging van Botnets
- Kennisdocument ten aanzien van de ontmanteling van Botnets

Ook zal het project verschillende rapportages opleveren:
- tussentijdse rapportages
- (min. 1) bestuurlijke rapportage[13]
- eindevaluatie

De beschreven kennisproducten zullen, onder vermelding van eventuele vertrouwelijke voorwaarden, actief verspreid gaan worden onder de politieregio's en andere vertrouwde binnenlandse en buitenlandse opsporingsdiensten. Deze kennisdocumenten kunnen door hen gebruikt worden indien ook bij hen Botnet-fenomenen een rol gaan spelen.

[13] De inhoud van een dergelijke rapportage zal tijdens het project duidelijk worden. Mogelijkheden op voorhand zouden kunnen zijn een dreigingsindicatie t.b.v. Nationaal Dreigingsbeeld (NDB), advisering aan het Ministerie van Defensie i.r.t. digitale dreigingen en/of tegenbewapening, advisering tot preventieve maatregelen binnen de NICC-bloemblaadjes, of direct aan het Ministerie van Binnenlandse Zaken t.b.v. preventieve maatregelen, bewustwordingscampagnes vanuit overheid, etc.

## 2.4 Aanpak

- Geef een uitwerking van de aanpak van de proeftuin
- Geef zo concreet en gedetailleerd mogelijk aan welke activiteiten verricht moeten worden om de gedefinieerde producten op te leveren en het omschreven doel en resultaat te behalen
- Geef daarbij (zo mogelijk) aan wie, wat, hoe en wanneer gaat doen
- Geef daarbij ook de activiteiten vanuit, als gevolg van en/of in samenspraak met het HRM-programma aan
- Besteed daarbij ook aandacht aan hoe ervaringen/producten worden gedeeld met eigen en/of andere deelnemende organisaties

In het schema op de volgende pagina zijn stapsgewijs de te nemen stappen binnen de aanpak omschreven. Fase 1 is hierbij op dit moment in een gevorderd stadium, en ook zijn reeds de eerste acties ondernomen met betrekking tot fase 2.

3.1 | 4.1

3.1 / 4.1

## 2.5 Planning

- Maak een planning in de tijd van de te verrichten activiteiten (grafische weergave)
- Nb 2.5 en 2.6 kunnen ook worden samengevoegd

Hieronder volgt op basis van het aangeleverde format de indeling van de hoofdfasen van het onderzoek uit paragraaf 2.4. Zoals uit het model ook af te leiden valt, zijn fase 1 en 2 al aangevangen. Echter wordt formeel aanvang genomen vanaf de officiële goedkeuring van het project door de Board Opsporing. Vanaf dat moment heeft de proeftuin naar verwachting een looptijd van 1 jaar, hetgeen THTC in zijn jaarplanning zal opnemen. Echter, omdat THTC een operationele eenheid van de DNR is, kan hiervan worden afgeweken indien operationele activiteiten van THTC en/of de DNR vanwege hogere prioriteit voorrang krijgen op het Botnet-project.

4.1

Nb Van deze fasering kan uiteraard worden afgeweken, afhankelijk van de concrete casuïstiek. Na elke fase vindt (in overleg met opdrachtgever) besluitvorming en eventueel heroverweging plaats.

Naast de hoofdfasen, zijn er voor de kortere termijn de volgende datums afgesproken:

- Aanbieding Concept Proeftuinplan aan
- Aanbieding Concept Proeftuinplanaan aan
  - < wijzigingen doorvoeren >
- Concept Proeftuinplan aan klaar voor eerste bespreking met PAC
  - < concept doormailen >
- Bespreking met
  - < wijzigingen doorvoeren >
- Oplevering definitieve versie Proeftuinplan
- Programmamanagersoverleg PAC-OM en PAC-Politie over Proeftuinen
- Besluitvorming van de proeftuin in de Board Opsporing

## 2.6 Mijlpalen

- Geef indien mogelijk de belangrijkste mijlpalen aan in de proeftuin (bijvoorbeeld go/no go besluit door opdrachtgever)
- Betrek hierin indien mogelijk ook belangrijke mijlpalen van andere belangrijke, buiten de proeftuin vallende projecten of activiteiten

Het project kent een aantal belangrijke mijlpalen welke belangrijk zijn voor het welslagen van het gehele project. Deze zijn:

1. Daadwerkelijke integratie van Botnet-datasets van externe partij(en). Deze mijlpaal geldt als het einde van 4.1 en is een vereiste om met 4.1 te kunnen starten
2.
3. 3.1 / 4.1

## 2.7 Benodigde resources en kosten

Hieronder zijn per geplande hoofdfase uit paragraaf 2.4 en 2.5 de geplande resources en kosten weergegeven. Om e.a.a. transparant declarabel te maken, is ervoor gekozen om de kosten vooraf verdeeld te specificeren voor PAC en OM.

4.1

- Geef aan wat de benodigde resources zijn; welke expertise, kennis en instrumenten zijn nodig voor deze aanpak en om de succesfactoren en leereffecten positief te beïnvloeden
- Geef daarbij aan wat korps/parket en partners zelf investeren in de proeftuin om succesfactoren en leereffecten positief te beïnvloeden (capaciteit, intelligence, expertise, ervaring, synergie in strategie, samenwerking, rapportage, procesbegeleiding, opleiding en training)

[14]

4.1

- Geef zo mogelijk aan wie of wat, wanneer, welke kosten met zich meebrengt en van welk budget dit kan (of zou moeten) worden betaald

## 2.8 Gevraagd budget

Toelichting voor het OM:
Over de toekenning van de OM budgetten aan de (regio)parketten heeft het College inmiddels beslist. Het (geoormerkt) budget kan worden aangewend voor de gekozen proeftuinen die een plan van aanpak hebben ingediend. In de P &C cyclus wordt verantwoording afgelegd over de feitelijke besteding van het budget aan een proeftuin. In het plan van aanpak (en de monitoring daarop) wordt gekeken of, en op welke wijze vanuit het budget capaciteit ingezet en op welke wijze die ingezette capaciteit een bijdrage heeft geleverd aan de proeftuindoelstellingen.

- Geef aan wat het gevraagde budget is (inclusief onderbouwing)

4.1

# 3. Projectorganisatie proeftuin

## 3.1 Opdrachtgever en opdrachtnemer

- Geef aan wie de opdrachtgever(s) is (zijn) van politie en OM
- Geef aan wie de opdrachtnemer(s) is (zijn) van politie en OM

De opdrachtgever vanuit de politie de proeftuin is 5.1 korpschef van het Korps Landelijke Politiediensten. De opdrachtgever van het Openbaar Ministerie is 5.1 , Hoofdofficier van Justitie van het Landelijk Parket.

Opdrachtnemer is Team High Tech Crime, Dienst Nationale Recherche. 5.1 zal tevens functioneren als projectleider van deze proeftuin.

## 3.2 Organogram proeftuin

- Geef in een schema aan hoe de projectorganisatie ten behoeve van de proeftuin en de eventuele besluitvormingsorganen is ingericht
- Plaats dit tevens in de context van de Intensiveringsprogramma's, te weten de inhoudelijke OM programma's GM, FINEC, Cybercrime en het HRM-programma en de Politie programma's FINEC, Cybercrime, Intelligence en Georganiseerde Hennepteelt

Nb Dit organogram kan geleverd worden door het Intensiveringsprogramma.

Omdat de proeftuin een operationeel onderzoek betreft, wordt er geen aspecifieke projectorganisatie opgezet. Er zal gebruik worden gemaakt van de bestaande besluitvormingsorganen en context waarbinnen de Dienst Nationale Recherche werkt. Het organogram daarvan, op basis van het reorganisatietraject Koers 2010, is weergegeven in figuur 6. Team High Tech Crime is voor het gemak hierin rood omcirkeld, evenals Team Digitaal en Internet (nieuwe benaming voor Team Digitale Expertise)

3.1 / 4.1

## 3.3 De projectgroep

Beschrijf de samenstelling en werkwijze van de gezamenlijke projectgroep die de proeftuin uitvoert. Geef daarbij in ieder geval aan:

- de samenstelling van de projectgroep
- de taken, verantwoordelijkheden en bevoegdheden van de projectgroep en de individuele deelnemers
- de verwachte inzet van de deelnemers gedurende het project
- hoe en op basis waarvan de besluitvorming tot stand komt
- of er sprake is van een begeleidingscommissie en wat daarvan de samenstelling is
- de rol van en de samenwerking met de (bovengenoemde) verschillende inhoudelijke programma's van OM en politie
- de rol van en de samenwerking met het HRM programma

Zoals reeds is genoemd in paragraaf 3.2, betreft de proeftuin een operationeel onderzoek binnen Team High Tech Crime. De projectgroep is daarmee feitelijk een operationele sectie van Team High Tech Crime, aangevuld met 2 personen (deeltijd) van Team Digitale Expertise voor ondersteuning en enkele maatwerktoepassingen. Het organogram van Team High Tech Crime ziet er als volgt uit.

3.1

In het linker onderdeel is te zien hoe beide operationele secties zijn opgebouwd. Een sectie wordt aangestuurd door een tactisch coördinator. Deze heeft dan ook binnen de proeftuin de dagelijkse operationele leiding, en legt verantwoording af aan de teamleider en de cybercrime-OVJ van het Landelijk Parket. Vanwege de proeftuinopzet wordt er nu dus een extra verantwoordelijke bijgeplaatst in de vorm van een projectleider. Hij zal primair het proces als totaal bewaken, alsmede de verantwoording richting de begeleidingscommissie rondom deze proeftuin. Deze begeleidingscommissie heeft de volgende leden:

5.1

Het Nationaal Intelligence Model (NIM) ligt ten grondslag aan deze proeftuin. Aan de ene kant is de proeftuin expliciet gericht op de verdere verbetering van de informatiepositie van de politie omtrent het fenomeen cybercrime. Aan de andere kant is de proeftuin gericht op het uitvoeren van opsporingsonderzoek door de Dienst Nationale Recherche en is daarmee per definitie volledig ingebed in de vigerende informatiestructuur van de politie. Te denken valt aan de centrale aansturing op het opsporingsonderzoek, informatieopdrachten worden afgeleid van informatiebehoeften. Briefing en debriefing zijn normaal, vanzelfsprekend onderdeel van de werkzaamheden. Speciale medewerkers van de Unit Informatie zijn decentraal op het team werkzaam. Zij zorgen voor de operationele informatievoorziening van en naar het team. Er is gekozen voor een decentrale werkplek vanwege het vakspecialisme wat High Tech Crime met zich meebrengt.

Op een later moment zal, zoals bij elke proeftuinorganisatie, ook nog formeel een Taskforce worden samengesteld. Dit is een orgaan waaraan geen directe verantwoording aan hoeft worden afgelegd, maar bijvoorbeeld kan fungeren als 'breekijzer' indien er problemen ontstaan in relatie tot de proeftuin, waar de projectgroep zelf niet uitkomt of die buiten de invloedssfeer van de projectleider liggen.

### 3.4 De borging van de proeftuin in de staande organisatie

- Beschrijf hoe de verantwoordelijkheidsverdeling tussen proeftuin en lijn loopt. Welke taken zijn een lijnverantwoordelijkheid en hoe vindt afstemming en wisselwerking met de proeftuinorganisatie plaats
- Besteed indien mogelijk aandacht aan de eventuele impact van het project op:
  - de staande organisatie
  - de financiën, de processen en (ICT)systemen
  - de medewerkers

3.1/4.1

## 3.5 Communicatie en overleg

- Geef aan hoe de communicatie en het overleg binnen de proeftuin geregeld is; wie communiceert, wanneer, waarover
- Geef aan hoe de communicatie en het overleg naar buiten over de proeftuin geregeld is

Aangezien het proeftuin-project een operationeel onderzoek van de DNR betreft, dient er door verschillende partijen terughoudend en bedachtzaam gecommuniceerd te worden over de inhoud van deze proeftuin. Externe communicatie zal, zoals bij alle onderzoeken van de DNR, louter plaatsvinden door of in uiterst nauwe samenwerking met het Landelijk Parket. Zowel de persvoorlichters van het LP als van de DNR zullen in een vroeg stadium op de hoogte worden gebracht van het lopende onderzoek, zodat zij toch adequaat kunnen reageren in het geval van onverwachte vragen vanuit bijvoorbeeld de pers. Echter, op een nog nader te bepalen moment, waarschijnlijk in een later stadium van het onderzoek, zal er gericht contact worden gezocht met de media, om via hen het publiek op de hoogte te stellen van de vorderingen. Het oogmerk hiervan zal mede gericht zijn op positieve aandacht, evenals voor waarschuwingen richting zowel (potentiële) verdachten als (potentiële) slachtoffers. Dit actieve persbeleid past ook in de gezamenlijke strategie van het LP en THTC. Echter zal het moment en de boodschap wel overwogen worden vastgesteld.

Binnen de politie zal ook slechts beperkt gecommuniceerd worden over het onderzoek. Om andere digitale onderdelen van Politie Nederland op de hoogte te houden, zal door de projectleider informatie verschaft worden tijdens het Operationeel Overleg Digitale Opsporing.

Binnen de proeftuinorganisatie zelf zal gecommuniceerd worden via de bestaande overlegmomenten zoals die in paragraaf 4.1 beschreven zijn.

# 4. Projectbeheersing

## 4.1 Voortgangsbewaking (achteraf)

- Geef aan hoe de voortgang wordt bewaakt (bijvoorbeeld door een logboek)
- Geef aan hoe over de voortgang aan de opdrachtgever wordt gerapporteerd
- Geef aan met welke frequentie over de voortgang wordt gerapporteerd
- Geef aan wie verantwoordelijk is voor de voortgangsbewaking

Omdat het project in zijn kern een operationeel onderzoek betreft, zal de dagelijkse aansturing plaatsvinden een tactisch coördinator van een sectie van Team High Tech Crime. De dagelijkse werkzaamheden zullen in de geijkte recherchesystemen als BVO worden bijgehouden. Ook zullen de bevindingen in de briefings wekelijks worden besproken en genotuleerd. Wekelijks zal de tactisch coördinator overleg voeren met de teamleider van Team High Tech Crime, alsmede met cybercrime OVJ van het Landelijk Parket. De projectleider van de proeftuin zal eens per 2 weken bij dit overlegmoment met justitie aanwezig zijn, om aldaar de voortgang van de betreffende fase, alsmede van het totale project te bewaken. Op basis van deze overlegmomenten zal deze proeftuin-projectleider 1 keer per 10 weken een voortgangsrapportage opstellen en deze doorsturen naar de opdrachtgevers en de begeleidingscommissie. Met deze begeleidingscommissie zal ook periodiek mondeling overleg worden gevoerd over de voortgang. De frequentie daarvan zal door de begeleidingscommissie zelf worden bepaald, maar op dit moment is het voorstel dit eveneens 1 keer per 10 weken te doen. In het volgende overzicht staat het bovenstaande nogmaals overzichtelijk weergegeven.

| Overleg | **Briefing operationeel onderzoek** |
|---|---|
| Persoon | - **Tactisch coördinator**<br>- **Medewerkers betreffende sectie van THTC** |
| Doel | Dagelijkse tactische en digitale aansturing van het onderzoek op basis van operationele feiten en ontwikkelingen |
| Frequentie | Dagelijks |

| Overleg | **Operationeel Overleg met Landelijk Parket** |
|---|---|
| Persoon (organisatie) | - **Tactisch coördinator sectie THTC**<br>- **Teamleider THTC**<br>- **Cybercrime OVJ LP**<br>- **Projectleider Proeftuin (1 per 2 weken)** |
| Doel | - Tijdens dit overleg wordt de OVJ op de hoogte gehouden van ontwikkelingen, en worden nadere tactische en juridische beslissingen genomen.<br>- 1 per 2 weken samen met projectleider: In het overleg wordt voortgang en planning van het project besproken en wordt besloten over de Project Issues die geen gevolgen hebben voor de planning, budget en kwaliteit |
| Frequentie | - 1 x per week |

| Overleg | **Begeleidingscommissie** |
|---|---|
| Persoon (organisatie) | - 51 - - - |
| Frequentie | Minimaal bij de start, voorts in de uitvoeringsfase door de begeleidingscommissie zelf nader te bepalen. Uitgangspunt is 1 maal per 10 weken. De projectleider zal tijdens dit overleg de voortgang van de proeftuin bespreken. |

## 4.2 Risicomanagement (vooruit denken)

- Geef aan welke risico's de uitvoering van de proeftuin kunnen belemmeren
- Geef aan welke risicobeheersende maatregelen de proeftuinorganisatie daartoe zal treffen
- Geef aan hoe het project met risico signalering -en beheer zal omgaan

31/41

De juridische complexiteit is deels een reden om de proeftuin te beginnen, echter vormt ook een risico. Vanwege de noviteit van de onderzoeksmethode, alsmede de noviteiten rondom mogelijke ontmantelingsstrategiën, bestaat de kans dat juridische bezwaren een eventuele veroordeling aan het eind van het onderzoek in de weg komen te staan. Om dit risico tot een minimum te beperken, zal het Landelijk Parket extra zorgvuldigheid betrachten bij juridische beslissingen, uit te schrijven machtigingen, etcetera. Waar nodig zal het Landelijk Parket extra kennis invliegen om zich daarmee maximaal te informeren over de juridische problematiek, om vervolgens deze kennis toe te passen binnen hun beslissingen. Feit blijft echter wel dat het een juridische verkenning zal blijven, en dat niet

uit te sluiten is dat op enig moment onzekere beslissingen moeten worden genomen. Het Landelijk Parket moet op zo'n moment bereid zijn meer risicovolle beslissingen te durven nemen. Eventuele tekortkomingen in bijvoorbeeld de wet worden daarmee ook des te meer duidelijk.

Een laatste risicofactor vormt de mogelijkheid dat er zich bij Team High Tech Crime onderzoeken aandienen waaraan een hogere prioriteit wordt toegekend. Hierdoor zou er capaciteit van het proeftuinonderzoek kunnen wegvloeien naar andere taken, waardoor er te weinig onderzoekscapaciteit zou kunnen overblijven om het onderzoek volwaardig te kunnen voortzetten. Tussen het Landelijk Parket, Team High Tech Crime en de Dienstleiding DNR zullen hierover nog nadere afspraken worden gemaakt om dit risico te beperken. Het risico kan echter nooit helemaal worden weggenomen, aangezien sommige prioriteiten of belangen altijd voor zullen blijven gaan, zoals bijvoorbeeld het recente SGBO Koninginnedag.

**BIJLAGE**

**Onderstaande informatie kan als hulpmiddel worden gebruikt bij de invulling van het plan van aanpak. Niet alle onderwerpen zijn in alle proeftuinen van toepassing.**

## A. Algemene aspecten.

Multidisciplinair werken:
Afhankelijk van het type onderzoek zal een aantal aspecten expliciet in de proeftuinopzet beschreven kunnen worden die van belang zijn bij de keuze voor de benodigde mensen en middelen (opzet van het multidisciplinaire team):

Van belang bij de multidisciplinaire inzet kan onder meer zijn[15]:

- Specifieke deskundigheid op het gebied van bejegening van slachtoffers (psychologen, kennis van culturen)
- Bestuurlijke context (verbinding naar het bestuur)
- Maatschappelijke context (verbinding en samenwerking naar en met maatschappelijke organisaties en/of private partijen)
- Logistiek van het proces ( in de opsporing/vervolging, maar ook later informatie uitwisseling en maken van afspraken met betrokken partners)
- Benodigde inhoudelijke kennis: (bv inschakelen financieel deskundige, bank- en/of notariële kennis, kennis van de "mores"van de handel)
- Expertise makelaar (kennis verzamelaar)
- Is er gedacht aan financiëel rechercheren (dus niet alleen t.b.v. "ontneming")

Aandachtspunten Internationale dimensie:

- samenwerking met het Landelijk Rechtshulpcentrum (Lirc) of een van de Internationale Rechtshulpcentra (irc's) om het rechtshulpverkeer, groot en klein (incl. internationale informatie-uitwisseling), zo goed mogelijk te laten verlopen. Benutten v.d. expertise (L)irc.
- Alert zijn op het juridisch instrumentarium: zijn er met de voor de zaak relevante landen voldoende juridische instrumenten (verdragen etc.) voor samenwerking?
- De Dutch Desk (de NL vertegenwoordiging bij Europol) van Europol vanaf het begin van het onderzoek (liefst nog in het stadium waarin het projectvoorstel wordt geschreven) raadplegen en zonodig inschakelen, o.a. ivm het maken van analyses en het blootleggen van verbanden naar andere landen.
- Via de Nederlandse vertegenwoordiging bij Eurojust, deze organisatie in een zo vroeg mogelijk stadium inschakelen. Dit in verband met het coördineren van m.n. justitiële rechtshulp en het maken van afspraken over in welk land het zwaartepunt van opsporing en vervolging zou moeten liggen?
- Serieus onderzoeken van de mogelijkheid om een Joint Investigation Team (JIT) via Europol op een zaak te zetten. Een JIT is een onderzoeksteam dat is samengesteld uit opsporingsambtenaren en officieren van justitie uit twee of meer EU-landen. Het instrument bestaat al geruime tijd, maar is nog weinig beproefd.
- BOOM betrekken bij de zaak i.v.m. zo vroeg mogelijk inzetten van (internationaal) ontnemen.
- Grensoverschrijdend/ euregionaal samenwerken toegespitst op de grensstreken.

[15] : Dit is een niet uitputtende opsomming van voorbeelden: niet alles is in elke proeftuin van belang

Politieke impact van een onderzoek
Indien sprake is van een politiek gevoelige zaak, dan dient vooraf nagedacht te zijn over de consequenties daarvan.

Communicatie traject lopende het onderzoek
Vooraf nadenken over de wijze en inhoud van communicatie. Waneer wel, wanneer niet, en zo ja wat en wanneer communiceren we met de ketenpartners en wat en wanneer met andere belanghebbenden en/of het publiek.

Toepasbaarheid van "best practices"
De toegepaste onderzoeksmethode en de resultaten uit de proeftuinen mogen lokaal gericht zijn, doch de methoden dienen ook opnieuw toepasbaar te zijn voor andere (lokale) onderzoeken. Resultaten worden zo snel mogelijk uitgeleerd in het land, eventueel door tussenkomst van de Tasforce voor het thema.

**B. Toelichting op de inhoudelijke criteria per thema (ontleend aan de intensiveringsprogramma's):**

**Cybercrime:**
In het thema Fraude op Internet zijn de volgende criteria van belang:

- Zijn er Nederlandse verdachten (kans op succes)?
- Is er inzet gewenst van innovatieve recherchetechnieken en opsporingsmethoden?
- Is er kans op ontwikkeling van nieuwe tools?
- Is er in een preventieve (of tegenhoud)strategie voorzien?
- Is er samenwerking met andere publieke of private partners gewenst?

In het thema ICT als doelwit zijn de volgende criteria van belang:
(Nader te bepalen) Eerste proeftuinen op dit thema zullen pas in 2009 starten.

9.1

Bovenstaande inhoudelijke criteria zijn geen voorwaarden voor het toekennen van een proeftuin maar aandacht voor deze punten is aan te bevelen omdat er naar wordt gestreefd deze criteria vertegenwoordigd te zien in een aantal van de te draaien proeftuinen over de gehele periode van het programma.