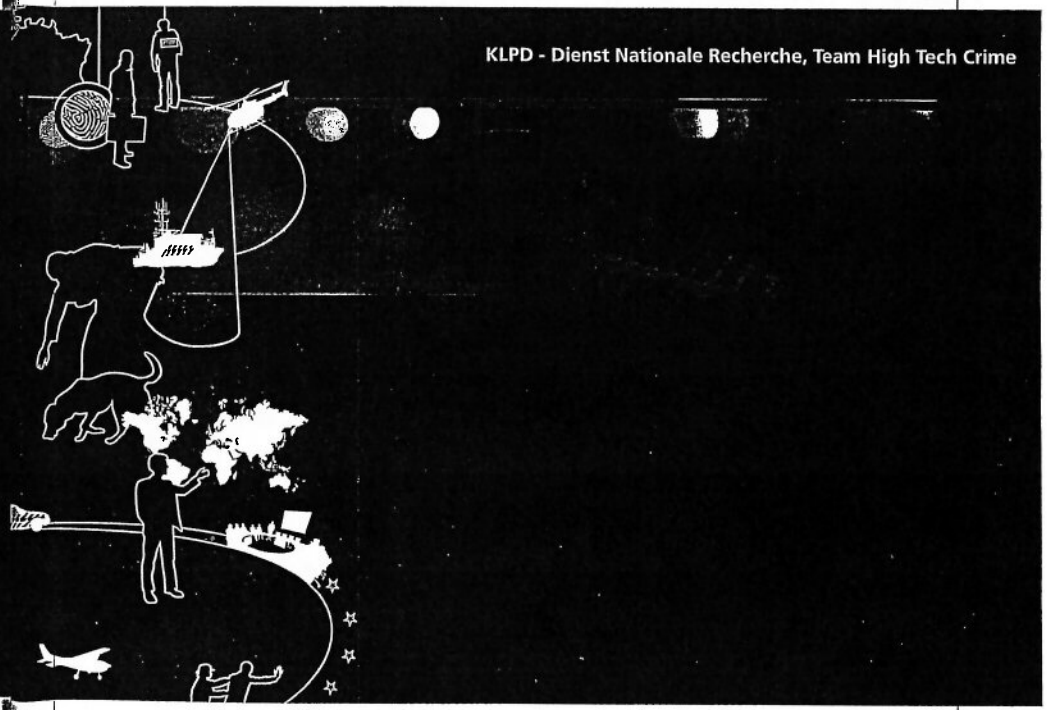
POLITIE
• Korps landelijke politiediensten

Kennisdocument Taurus

Ervaringen uit een proeftuin



KLPD - Dienst Nationale Recherche, Team High Tech Crime

«waakzaam en dienstbaar»

POLITIE
• Korps landelijke politiediensten

Kennisdocument Taurus

Ervaringen uit een proeftuin

KLPD - Dienst Nationale Recherche, Team High Tech Crime

«waakzaam en dienstbaar»

POLITIE
• Korps landelijke politiediensten

Uitgave

Korps landelijke politiediensten (KLPD)
Dienst Nationale Recherche, Team High Tech Crime
Hoofdstraat 54
3972 LB Driebergen
Postbus 11
3970 AA Driebergen
Driebergen, maart 2011

Colofon

Tekst 5.1

Foto omslag iStockphoto
Druk Repro KLPD
Opmaak OSAGE/communicatie en ontwerp

Inhoud

1 Inleiding

Het Kabinet heeft voor de bestrijding van cybercrime, financieel-economische criminaliteit en georganiseerde misdaad gelden vrijgemaakt[1]. De politie en het Openbaar Ministerie (OM) hebben zich gecommitteerd aan de intensiveringprogramma's die daaruit voort moesten komen[2].
Zo is in het Strategiedocument 2009-2011 tussen het Landelijk Parket (LP) en Team High Tech Crime (THTC) overeengekomen dat binnen de aanpak van cybercrime meer aandacht uit zal gaan naar de aanpak van botnets.

Botnet
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, het middels key logging stelen van persoonlijke gegevens of het omleiden van internet-bankierverkeer.

Het THTC ontwierp een aanpak gericht op het verbeteren van de informatiepositie van de politie ten aanzien van botnets, om van daaruit concrete opsporingsonderzoeken uit te kunnen voeren

4.1

Deze proeftuin droeg de naam Taurus.

Het doel van Taurus was drie concrete doelstellingen te bereiken op het gebied van publiek-private bestrijding van botnets en daar werkenderwijs meer over te leren. Die doelstellingen waren:
1. Versterken van de informatiepositie ten aanzien van botnets, door zicht te krijgen op minimaal 750 botnets;
2. Gericht repressief rechercheonderzoek naar 3 criminele botnets, leidend tot identificatie van minimaal 1 verdachte per botnet;

1 Dit is beschreven in het veiligheidsprogramma "Veiligheid begint bij Voorkomen"
2 Dit is beschreven in de stukken "gezamenlijke landelijke prioriteiten politie 2008-2011" en Visie en plan van aanpak Programma Cybercrime

3. Gerichte preventieve maatregelen ter bestrijding van botnets, leidend tot de uitschakeling van minimaal 80% van bij het THTC bekende in Nederland gehoste Command & Control (C&C) servers.

Het opleveren van een evaluatiedocument en kennisdocumenten behoren ook tot de doelstellingen van Taurus. Het plan van aanpak noemt vier gebieden waarop een kennisdocument moet verschijnen, te weten Publiek Private Samenwerking (PPS), decryptietechnieken, juridische aspecten en ontmanteling van botnets.

4.1

Scope

Dit kennisdocument is opgesteld naar aanleiding van de proeftuin Taurus. Uit het Taurusproject is het opsporingsonderzoek Tolling ontstaan, wat leidde tot de ontmanteling van Bredolab. Wanneer het ten goede komt aan het duidelijk beschrijven van de leereffecten van Taurus, is ook de doorstap gemaakt naar Tolling.

Doelgroep en gebruik kennisdocument

Het kennisdocument is in eerste instantie bedoeld voor het vastleggen van kennis voor de eigen organisatie van het THTC en het LP. Voorts kan (een deel van) het document interessant zijn voor de bij het project betrokken partijen. Vanuit de nationale rol van het KLPD kan (een deel van) het document tenslotte ter informatie verspreid worden aan (bijvoorbeeld Bureau's Digitale Expertise van) regiokorpsen.

Niet alle beschreven informatie is voor alle partijen nieuw. De context waarin deze informatie is opgedaan, is dat wel. Het heeft waarde op zich, om het op geordende wijze vast te leggen voor toekomstig gebruik in een soortgelijke situatie. De kans is namelijk aanwezig dat in de nabije toekomst vaker de PPS-constructie zal voorkomen voor het bestrijden van botnets of andere vormen van cybercrime.

Totstandkoming

Het kennisdocument is tot stand gekomen door documentenonderzoek en interviews. De documenten zijn door het THTC beschikbaar gesteld en

interviews zijn gehouden met vrijwel alle betrokken partijen (zie de bijlagen voor een overzicht van schriftelijke bronnen en respondenten).

Opbouw van het kennisdocument

Dit document bevat voor elk kennisonderwerp een hoofdstuk: Publiek Private Samenwerking (hoofdstuk 2), juridische aspecten (hoofdstuk 3), tooling (hoofdstuk 4), decryptie (hoofdstuk 5) en ontmanteling van botnets (hoofdstuk 6). Per onderwerp wordt ingegaan op de relevantie van het onderwerp, de doelstellingen, bevindingen, conclusies en aanbevelingen.

2 Publiek Private Samenwerking

De bestrijding van botnets kan niet door een partij alleen worden gedaan. Samenwerking, bij voorkeur internationaal, is noodzakelijk voor een effectieve opsporing en bestrijding van botnets. Taurus is opgezet als Publiek Private Samenwerking (PPS). Dit hoofdstuk gaat in op de redenen en opzet van de PPS, de toegevoegde waarde van samenwerking voor de partners en de gebruikte communicatiemiddelen.

2.1 Relevantie Publiek Private Samenwerking voor Taurus

De basis van Taurus is een PPS waarin private partijen en publieke partijen met en zonder opsporingsbevoegdheden samenwerken. Een PPS wordt opgericht met een bepaald doel voor ogen. Het doel van samenwerking in Taurus is:

- versterking van de informatiepositie ten aanzien van botnets;
- verdeling van de capaciteitsdruk;
- gezamenlijke bescherming van de vitale infrastructuur; en
- samenwerking voor het gezamenlijk opwerpen van drempels voor hightech-criminelen.

2.2 Lessen uit de proeftuin Taurus

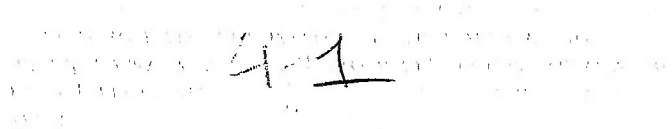
Selectie van deelnemers

De samenstelling van de groep verschilt per samenwerkingsverband. Bij de samenstelling is het doel van de PPS van belang, dit bepaalt grotendeels de groepssamenstelling, net als overigens de vereiste kennis en capaciteiten.

Het ligt voor de hand om bij de selectie van partijen eerst te kijken naar bestaande contacten, waarmee al in enige vorm met succes wordt samengewerkt. Het daaruit voortvloeiende onderling vertrouwen is belangrijk om het nieuwe samenwerkingsverband een snelle start te geven.

Deze aanpak volstaat niet altijd voor een volledige dekking van het speelveld en ondervangt ook niet het risico dat persoonlijke contacten en voorkeuren een

belangrijker rol spelen dan het doel van de samenwerking. Voor optimale dekking en evenwicht tussen partijen is het belangrijk met een kernteam te overleggen over het soort partijen dat nodig is en de verschillende mogelijkheden.



Evenwicht tussen de partijen is nodig om te zorgen dat niet één partij door zijn omvang of cruciale expertise een te dominante rol gaat spelen en andere 'wegdrukt'. Dit laatste kan namelijk onbedoeld leiden tot afhaken van partijen.

De partijen die deelnamen aan Taurus kwamen uit vier groepen, 1) de publieke law enforcement, 2) overige publieke organisaties, 3) service providers en 4) IT Security.

Redenen om samen te werken voor private partijen zijn divers

Deelnemers moeten ten eerste voldoende intrinsiek gemotiveerd zijn om een bijdrage te leveren aan het (maatschappelijke) doel. Dit geldt zeker voor private partijen, die normaal gesproken betaald krijgen voor hun diensten. Voor publieke organisaties geldt, dat zij vanuit hun publieke rol doorgaans al het maatschappelijk doel dienen, zij het vanuit een specifieke eigen invalshoek.

De private partijen die deelnamen aan Taurus deden dit in de eerste plaats vanwege het maatschappelijke belang. Zij vonden dat zij aan het bestrijden van botnets een bijdrage konden en moesten leveren.

Uit Taurus kunnen de volgende motieven van private partijen voor deelname aan een PPS voor opsporingsonderzoek worden gehaald:

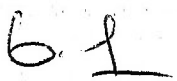
- Het delen van kennis en gezamenlijke inzet van capaciteit leidt tot synergie, waardoor het gemeenschappelijk doel dichterbij komt;
- Een concreet doel en concrete aanpak spreken aan;
- Door deelname ook mede sturing kunnen geven aan ontwikkelingen.
- Door de samenwerking ontstaan praktijkervaringen en inzichten over wie wat kan en wie waar in de dagelijkse praktijk mee bezig is;

- Deelname aan een samenwerking met nationale opsporingsinstanties verleent een soort kwaliteitsstempel aan een bedrijf. Het ondervangt ook kritische vragen van klanten omdat je door de deelname transparant bent over je bedrijfsbeleid.
- Opdoen van kennis door gaande het traject te leren van anderen en door eigen praktijkervaring;
- Business development, voorinvesteren om later kans te maken op betaalde opdrachten, binnen of buiten de PPS.

Samenwerking is niet per definitie win/win

Naast de hierboven beschreven win/win situatie kan samenwerking ook leiden tot een win/loss of loss/loss situatie. Dat wil zeggen dat partijen juist iets verliezen door in zee te gaan met elkaar.

Ten eerste komt dat door risico's vanuit concurrentieoverwegingen. Bij het verstrekken van gegevens kan bijvoorbeeld een bepaald informatievoordeel uit handen worden gegeven.



Ten tweede kan publiciteit negatief werken en leiden tot imagoschade, bijvoorbeeld als het resultaat beperkt is of niet goed wordt ontvangen. Daarbij kan 'het grote publiek' anders reageren dan de eigen klanten of partners in de relatief kleine cyberwereld.

Ten derde kan een investering om mee te doen op niets uitdraaien door een verandering van inzichten of scope. Dat kan ertoe leiden dat slechts een enkele partij uiteindelijk baat heeft bij een PPS en andere niet. Bewaking van scope is dus niet alleen noodzakelijk vanuit oogpunt van het project, maar ook om partijen binnenboord te houden.

Ten vierde betekent deelname dat voor die tijd geen commerciële inzet mogelijk is wat leidt tot inkomstenvermindering. Private partijen verwachten een goede balans tussen inspanningen en opbrengsten. De opbrengsten kunnen ook van immateriële aard zijn of pas op termijn resultaat geven.

Openheid stimuleert samenwerken

Proactieve openheid vanuit de overheid werkt stimulerend voor de PPS en wekt vertrouwen. Oók openheid over beperkingen en onzekerheden wordt als prettig ervaren. Het is namelijk niet nodig dat van tevoren alle mogelijkheden uitgeplozen zijn en vastliggen. Dit is beter dan het onder het tapijt vegen van onduidelijkheden.

6.1

Bespreek de manier van samenwerken en elkaars win/loss punten

In een convenant worden duidelijke *Rules of Conduct* opgesteld, waarin beschreven waarin afspraken over de samenwerking worden opgesteld. Het gaat om zaken als tot hoe ver *law enforcement* kan gaan met het opvragen van gegevens, wat met deze gegevens kon gaan gebeuren, de wijze van communiceren naar de pers, duidelijkheid over de juridische grenzen en mogelijkheden van andere partners. Elementen kunnen naar behoefte worden opgenomen.

Bij het vormgeven van de Rules of Conduct is van belang dat verwachtingen uitgesproken worden en voor ieder helder is waar de afbreukrisico's zitten voor iedereen. Voor private partijen is bescherming van concurrentiegevoelig intellectueel eigendom belangrijk.

6.1

In het door Taurus gebruikte convenant zaten overigens weinig harde verplichtingen voor de private partijen. De afspraken waren "niet in rechte afdwingbaar", behalve de bepalingen ten aanzien van de geheimhouding en de beveiliging[3]. De meeste partijen zagen het convenant dan ook meer als een intentieverklaring.

3

6.1

Andere belangrijke onderwerpen om afspraken over te maken zijn (onder andere) publiciteit en de regie erop, geheimhouding, eventuele vergoeding voor diensten, delen van informatie en contactpersonen.

Veranderingen in de samenstelling van partijen en deelnemers

Samenwerking tussen organisaties is sterk afhankelijk van individuele personen. Wisseling van de wacht is dan ook altijd een aandachtspunt. Het kan op zijn best leiden tot vertraging in activiteiten, maar ook tot volledige uitval van de partij. Het voldoende kennen van de andere partijen en op de hoogte zijn van hun interne dynamiek is aanbevelenswaardig, opdat verrassingen zo beperkt mogelijk blijven.

Een verminderde inbreng hoeft overigens niet negatief te zijn als deze partijen als een 'outer circle' betrokken blijven en hun mening vanuit hun invalshoek kunnen geven.

Beperk complexiteit in organisatie en materie

Als werken met een PPS nieuw is, dan is het verstandig om te starten met niet al te complexe doelstellingen. Het werken in een groot en publiek-privaat verband is dan al een leertraject op zichzelf.

> Taurus richtte zich op een eenvoudige vorm van botnets. De opzet van de samenwerking was complex. De beperking tot 'eenvoudige' botnets maakte het (onbedoeld) mogelijk om meer aandacht aan de complexiteit van het nieuwe samenwerkingsverband met zoveel spelers te besteden.

Bij de opzet van een PPS is de beheersing en beperking van het aantal complexe elementen een belangrijke succesfactor.

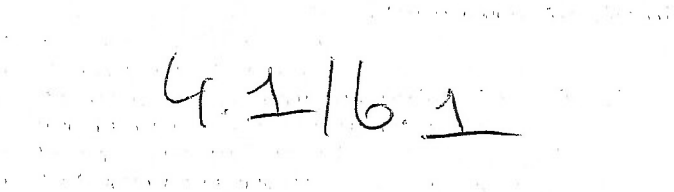
Kies een mix van communicatiemiddelen die aansluiten bij behoeftes

Veranderingen in het project, zoals groei of voortschrijdende fasering, kan leiden tot andere vormen van interactie tussen de partijen. De ervaring van Taurus leert, dat persoonlijk contact het meest effectief is. De investering in (reis-)tijd verdient zich bijna altijd terug. In Taurus beproefde middelen zijn:

- Persoonlijk contact via (korte) meetings op locatie of telefoon. Dit stimuleert de kennisuitwisseling goed. Naast inhoudelijke kennisuitwisseling kunnen ook juridische, technische en organisatorische issues die zich voordoen snel met face to face contact opgelost worden;

- Expertmeetings over specifieke onderwerpen met geselecteerde personen. Een lijfelijke 'kick-off' draagt ook bij aan het samenwerkingsgevoel en verlagen het de drempel om later contact op te nemen en gegevens uit te wisselen.

De expertmeetings droegen in Taurus sterk bij aan het ontstaan van vertrouwen en samenwerking omdat nu een gezicht bij een naam geplaatst kon worden. Zo werd duidelijk welke persoon wat kon leveren. Het verlaagde de drempel om contact op te nemen of om gegevens uit te wisselen. De communicatiemiddelen werden veel ondersteund door technische hulpmiddelen, zoals het forum en de portal. Deze digitale hulpmiddelen werden echter weinig gebruikt.



Juist bij dergelijke middelen is het vinden van de balans tussen gebruiksgemak en beveiliging precair. Enerzijds mag niet zomaar alles 'op straat' komen te liggen, anderzijds moeten mensen het forum, de file of de mail wel lezen. Niet iedereen haalt consequent files op van een beveiligde fileserver, of participeert in digitale fora, zo blijkt ook uit Taurus.

Een verwant communicatiedilemma is het verschil tussen halen en brengen. Als je graag wilt dat mensen je boodschap of informatie tot zich nemen, maak dan de drempel voor kennisname zo laag mogelijk.

Het bepalen van de communicatiestrategie en bijbehorende middelen is situatiegebonden. De omvang, diversiteit, behoeftes en geografische spreiding (en dus tijdsverschillen) van de deelnemers zijn factoren om rekening mee te houden. Dit kan ook vraaggestuurd gebeuren door de vraag "hoe willen we met elkaar communiceren en data delen" te stellen in het samenwerkingsverband.

Een volgende samenwerking na Taurus moet scherp zicht hebben op de communicatie met de betrokken partijen. De behoefte aan samenwerken en interactie verschilt tussen partners en kan verschuiven in de tijd. Het houden van meer expertmeetings omdat deze bij Taurus een succes bleken is geen garantie voor succes bij een volgend project!

Verken duurzame vormen van PPS

Bij de opzet van duurzame samenwerking kan gestreefd worden om een PPS - zoals Taurus te institutionaliseren. In het Verenigd Koninkrijk en de Verenigde Staten zijn *good practicus* bekend die kunnen dienen als voorbeeld van een structurele PPS. Er zijn goede kansen om hier naar toe te groeien. De partijen noemden enkele suggesties voor een versteviging van de samenwerking:

- Laat private partijen een deel van het (voor)onderzoek of analyse uitvoeren. Zo kunnen zij een eerste scan op malware uitvoeren. Zij kunnen bijvoorbeeld bij het monitoren van hun netwerkverkeer snel zicht krijgen op de C&C servers. Hierdoor is het niet of minder nodig zelf te investeren in opsporingstools;
- Gebruik van data van al lopende onderzoeken en trajecten bij andere partijen. Hierin kan aansluiting worden gezocht met de ISP's ter aanvulling op de rol die de politie kan innemen;
- Gebruik van open source intelligence zoals open bronnen van malware verspreiders als informatiebron en als startpunt van een (voor)onderzoek;
- Wissel operationeel personeel uit om inzicht te krijgen in elkaars doelen en om sneller gewenste informatie te delen: "nothing beats the phonecall to one's own organisation". In Taurus is hier goede ervaring mee op gedaan zoals bij de tweede expertmeeting, in de samenwerking met de Universiteit Aken en in de samenwerking tussen het KLPD en GOVCERT.NL;
- Overweeg een hoge functionaris van een private partner in de begeleidingscommissie op te nemen om evenwicht tussen partijen in de sturing te krijgen;
- Stel een plan op om te bepalen waar je in de samenwerking met andere partijen op termijn naar toe wilt groeien.

2.3 Conclusie

Door deelname aan Taurus groeide en verstevigde het netwerk van elk van de partners. Taurus bleek een waardevolle katalysator voor samenwerking elders en het leggen en verstevigen van contacten. Het investeren in warme relaties, oog hebben voor elkaars *'what's in it for me'* en concreet werken aan concrete resultaten zorgen voor de echte meerwaarde. Indien deelname binnen afzienbare termijn weinig oplevert zal dit intern steeds moeilijker te verdedigen zijn. Een samenwerking betekent niet dat alle activiteiten met gesloten beurs worden uitgevoerd.

Taurus leert dat korte, afgebakende trajecten helpen om de samenwerking levensvatbaar en flexibel te houden. De samenstelling van de partijen in het samenwerkingsverband kan veranderen gedurende het traject. Het toevoegen van partijen of veranderen van de vertegenwoordigers van partijen kan contraproductief werken. Persoonlijk contact en eerder gedeelde inzichten, gesprekken en informele afspraken zijn moeilijk uit te wisselen. PPS is dus ook een kwestie van persoonlijke contacten. Mensen doen zaken met mensen.

Ondanks formele afspraken is de uitvoering een kwestie van de inzet van individuen. Zo bleek de meest effectieve vorm van communicatie de (korte) meetings of contact via mail of telefoon. De conclusie is dat ook als sprake is van contact tussen organisaties, uiteindelijk mensen met mensen zaken doen.

In een volgende samenwerking zal zo snel mogelijk gezocht moeten worden naar een gemeenschappelijk, concreet doel. Daarbij kan de samenwerking beperkt blijven tot partijen die in het concrete geval bij willen dragen. De inbreng zal per partij en per project verschillen. Wel kunnen andere partijen op de hoogte gehouden worden en zo betrokken blijven.

Aanbevolen wordt een duidelijker strategie te ontwikkelen om kennis of inzet zelf te leveren, in te kopen of te verwerven door coproductie. Daarbij zal in de projectopzet en budgettering ruimte voor de inhuur van externe expertise of vaardigheden opgenomen moeten worden. Hierbij kan gebruik gemaakt worden van een stakeholderanalyse, waarmee een groeipad voor de lange termijn opgesteld kan worden. Processturing verdient hierbij de volle aandacht, zeker bij grotere, multidisciplinaire samenwerkingsverbanden met meerdere projectdoelen.

3 Juridica

De proeftuin Taurus werd mede ingericht vanwege enkele juridische vraagstukken over de uitvoering en toepassing van wettelijke mogelijkheden ten aanzien van de opsporing en ontmanteling van botnets.

3.1 Relevantie juridica voor Taurus

Een nevendoel van de proeftuin Taurus was de juridische grenzen te verkennen en bij te dragen aan de jurisprudentie ten aanzien van de bestrijding van botnets.

- Ten eerste ten aanzien van de onderzoeksmethode en ontmantelingstrategieën. Het is namelijk niet altijd duidelijk of de (huidige) wetgeving afdoende is om misdrijven in het cyberdomein op te sporen en te vervolgen.
- Ten tweede ten aanzien van de consequenties. Niet alle consequenties en onderzoeksrichtingen waren op voorhand in te schatten. Dit vroeg om flexibiliteit van het LP en partners om te kunnen anticiperen op voortschrijdend inzicht. Van tevoren was duidelijk dat het karakter van de juridische verkenning mogelijk op enig moment om beslissingen met onzekere uitkomst zou vragen. Het LP was bereid deze risico's te nemen.

Het plan van aanpak benoemde vier innovatieve elementen van de juridische aanpak:

- Welke strafvorderlijke bevoegdheden zijn nodig voor de gegevensverwerking?
- Wat is de grondslag van een eventueel opsporingsonderzoek?
- Wat is de bevoegdheid bij het 'overnemen' van een botnet?
- Wat zijn de mogelijkheden tot opsporing op afstand in geautomatiseerde werken die zich in het buitenland bevinden?

De juridische complexiteit vormde een risico voor het uiteindelijke resultaat van de proeftuin. De kans bestond dat juridische bezwaren een eventuele veroordeling in de weg zou staan. Het projectteam toetste daarom de opzet van de proeftuin bij de Landelijk Officier van Justitie Cybercrime en Interceptie, de betrokken privacyfunctionarissen van het Korps Landelijke Politiediensten (KLPD), het Landelijk Parket (LP) en de privacy desk van het Parket Generaal. Het convenant is vormgegeven door een onafhankelijk juridisch adviesbureau.

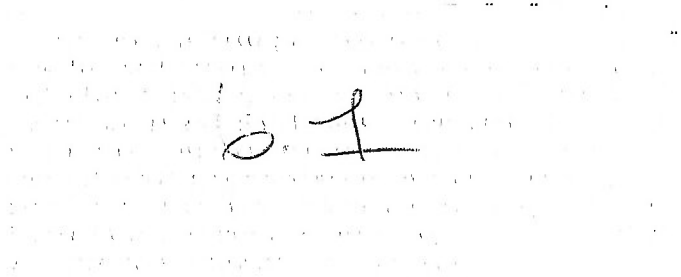
Op deelaspecten is informeel *gesparred* met een inhoudelijk ingevoerde rechter-commissaris.

Bij het schrijven van dit rapport is specifieke jurisprudentie naar aanleiding van Taurus (of Tolling) nog niet ontstaan. Zolang er nog geen zaken uit Taurus (of Tolling) voor de Nederlandse rechter zijn gekomen (of wetgeving aangepast is), is het onzeker of de gevolgde interpretaties ook stand kunnen houden. De conclusies moeten dan ook in dat licht bezien worden.

3.2 Lessen uit de proeftuin Taurus

Verkrijgen van gegevens vraagt om een vordering

Gegevens moeten op rechtmatige wijze verkregen en verwerkt zijn. Het vorderen van gegevens is noodzakelijk om de gegevens te kunnen gebruiken in een strafzaak. Het staat een opsporingsambtenaar of officier van justitie niet zonder meer vrij om van derden te vragen om op vrijwillige basis gegevens te verstrekken[4]. De wenselijkheid van de vordering is verwoord in het Handboek voor de Opsporingspraktijk[5]: "Indien in het belang van het opsporingsonderzoek gegevens moeten worden verkregen, dan geldt als uitgangspunt dat de wettelijke regeling van de bevoegdheden tot het vorderen van gegevens wordt toegepast. Dit geldt ook als daartoe strikt genomen geen noodzaak bestaat omdat de gegevens niet vallen onder de Wet Bescherming Persoonsgegevens (WBP), zoals algemene bedrijfsgegevens."



4 Dit uitgangspunt staat ook bekend als "de wet Mevis".
5 Openbaar ministerie, Handboek voor de Opsporingspraktijk (2009), deel I, hoofdstuk 2 bijzondere opsporingsbevoegdheden, Blz 397

Vorderen heeft een connotatie van ongelijkheid in zich: de politie vraagt niet, maar eist gegevens. De politie kan de vordering naar private partners ook positioneren als "slechts een juridische formaliteit" om vriendschappelijk verkregen gegevens te kunnen verwerken.

Het monitoren van botnets kan op basis van Stelselmatige Inwinning

Een bevel voor stelselmatige inwinning (art. 126qa WvSr) is een juridische basis voor de informatieverzameling en veredeling van gegevens over botnets. Deze bevoegdheid kan worden omdat sprake is van criminele activiteiten in georganiseerd verband[6]. Het proces-verbaal om het bevel stelselmatige inwinning aan te vragen in Taurus, onderbouwde dat als sprake is van het gebruik van botnets al snel sprake is van een georganiseerd verband. De aanleiding waren misdrijven onder artikel 138A, 138B, 139D, 139e, 161sexies en 350A WvSr.

Artikel 126qa lid 1 Wetboek van Strafvordering
"In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onderdeel b, zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar, stelselmatig informatie inwint over een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in het georganiseerd verband beramen of plegen van misdrijven."

Delen van gegevens kan op basis van een convenant

Het delen van politiegegevens met partijen die niet bij name genoemd worden in de Wet of Besluit politiegegevens kan op basis van een convenant onder artikel 20 Wet Politiegegevens (Wpg).

6 Dit is omschreven in het PV "omschrijving georganiseerd verband". De aanleiding waren misdrijven onder artikel 138A, 138B, Hier hoeft niet altijd gebruik van gemaakt te worden. Binnen Taurus was dit bijvoorbeeld niet altijd relevant, omdat het gegevens van partners betrof, zodat zij hun eigen gegevens retour zouden krijgen. Verder beperkte de verstrekking zich beperkt tot de overdracht van IP adressen en samples en in mindere mate veredelde gegevens. 139D, 139e, 161sexies en 350A WvSr.

Artikel 20 Wet Politiegegevens

1. *De verantwoordelijke kan, voor zover dit met het oog op een zwaarwegend algemeen belang noodzakelijk is ten behoeve van een samenwerkingsverband van de politie met personen of instanties, in overeenstemming met het op grond van de Politiewet 1993 bevoegd gezag, beslissen tot het verstrekken van politiegegevens aan die personen en instanties voor de volgende doeleinden:*

a. *het voorkomen en opsporen van strafbare feiten;*
b. *het handhaven van de openbare orde;*
c. *het verlenen van hulp aan hen die deze behoeven;*
d. *het uitoefenen van toezicht op het naleven van regelgeving.*

2. *In de beslissing, bedoeld in het eerste lid, wordt vastgelegd ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, alsmede het doel waartoe dit is opgericht, welke gegevens worden verstrekt, de voorwaarden onder welke de gegevens worden verstrekt en aan welke personen of instanties de gegevens worden verstrekt.*

6.1

6.1

Taurus is uitgevoerd onder Titel V, een opsporingsonderzoek naar een georganiseerd verband.

Een deugdelijke juridische grondslag onder de onderzoeken was nodig om geen risico's te lopen in een eventuele strafzaak. Er zijn grofweg twee juridische opties om een onderzoek te starten. De eerste optie is een verkennend vooronderzoek. Deze heeft als nadeel dat bij een eventuele zaak alle data uit het vooronderzoek vrijgegeven moet worden. Deze data wordt dan feitelijk voor andere onderzoeken minder waard.

De tweede optie is de verzameling van gegevens te zien als het stelselmatig inwinnen van informatie (SI), onder titel V (art 125i) WvSv. Het voordeel hiervan is, dat er één algemeen onderzoek kon starten, waaruit diverse afzonderlijke opsporingsonderzoeken voort kunnen komen (die dan vallen onder Titel IVa). De data uit het eerste onderzoek blijven bruikbaar voor vervolgacties. Deze werkwijze geeft meer vrijheid dan een verkennend vooronderzoek.

Een vuistregel om te bepalen welk juridisch regime gebruikt kan worden voor het verzamelen van informatie is de hand wat je ziet (en doet) met die tool.

7

6.1

Een IP adres is niet altijd een persoonsgegeven

Bepalend voor de toepassing van de privacywetgeving is de vraag is of een IP-adres als persoonsgegeven gezien moet worden. Gezien de doelbinding van Taurus, waaronder het uitvoeren van een gericht onderzoek naar personen, besloten het OM en het THTC de IP adressen te verwerken als persoonsgegevens, onder de Wet Politiegegevens.

Uiteindelijk is een IP-adres namelijk, al dan niet in combinatie met andere gegevens, te herleiden tot een persoon. Dit is ook één van de doelen van het onderzoek. Het College Bescherming Persoonsgegevens (CBP) geeft dan ook aan dat de een IP-adres in veel gevallen, maar niet altijd een persoonsgegeven is.

"De Registratiekamer is van mening dat een volledig IP-adres in veel gevallen als persoonsgegeven moet worden beschouwd. Hierdoor vallen verwerkingen van IP-adressen over het algemeen onder de reikwijdte van de privacy-wetgeving. De verschijningsvorm van het IP-adres is hier echter bepalend voor."[8]

Omdat het monitoren van botnets, zoals bij Taurus, het verwerken van persoonsgegevens impliceert, gelden wettelijke privacy plichten. Dit omvat het aanmelden van een gemeenschappelijke verwerking bij het CBP.

8 Brief College Bescherming Persoonsgegevens (toen Registratiekamer), d.d. 19 maart 2001, kenmerk z2000-0340

Rerouten en sinkhole

Als middel voor het neerhalen van botnets kan vooralsnog geen gebruik gemaakt worden van een sinkhole. De algemene vraag naar een juridische oplossing voor deze mogelijkheid ligt al sinds 2008.[9]
In het concept voor een zogenaamde '*honey sinkhole*' wordt een bepaald (.nl) adres gerouteerd waarmee verkeer omgeleid wordt naar een sinkhole voor verdere bestudering. De huidige wetgeving voorziet echter niet in een dergelijke opsporingsbevoegdheid.

Sinkhole
Er zijn verschillende manieren om een sinkhole in te richten. Over het algemeen werken sinkholes door het '*spoofen*' van de DNS servers. De adressen in de DNS server worden aangepast en valse adressen worden ingegeven. Wanneer dit adres wordt aangeroepen retourneert de DNS sinkhole geen adres waardoor de aanvraag 'verdwijnt' of geeft een ander adres waardoor de aanvraag wordt omgeleid. Hierdoor zal geen contact gelegd kunnen worden met de oorspronkelijke target host.

3.3 Conclusie

Taurus zocht als proeftuin de grenzen op en stelde een aantal specifieke vragen ten aanzien van juridische mogelijkheden. De gemaakte juridische keuzes zijn nog niet getoetst bij een rechter omdat Taurus noch Tolling tot een zaak heeft geleid in Nederland. Niet alle vragen zijn uiteindelijk in de proeftuin beantwoord. Om meer projecten als Taurus te kunnen draaien is grotere bekendheid van de wettelijke mogelijkheden wel noodzakelijk.

Jurisprudentie is niet de enige vorm om een idee te vormen over de rechtmatigheid van handelen. Andere rechtsbronnen kunnen ook bijdragen aan het vormen van een (gedeelde) mening over het gebruik van juridische middelen, zij het dat deze juridisch minder sterk zijn dan een rechterlijke uitspraak of wetgeving. Daarbij kunnen andere vormen van discussie en manieren om een richting te onderbouwen mogelijk vraagstukken breder benaderen.

9 Zie Inventarisatie ervaring wet- en regelgeving cybercrime, KLPD, 22 september 2008. Hierin wordt 'spoofing' genoemd als gewenste opsporingsbevoegdheid, net als het in beslag nemen van IP adressen of domeinnamen.

Wanneer een samenwerking als Taurus vaker wordt toegepast is hergebruik en aanpassing van de al bestaande convenanten mogelijk. \

6.1

4

Voor het opbouwen en onderhouden van een goede informatiepositie over botnets zijn geautomatiseerde hulpmiddelen noodzakelijk. Dit is onder andere zo vanwege het grote aantal botnets dat actief is en de grote dynamiek in commando's. In deze paragraaf gaan we in op de rol die tooling kan vervullen bij een PPS ter bestrijding van hightech crime.

4.1

4.1

4.2 Lessen uit de proeftuin Taurus

4.1

4.1

3.1 / 4.1

4.3 Conclusie

3.1 / 4.1

5

5.1

3.1 / 4.1

5.2 Lessen uit de proeftuin Taurus

3.1 / 4.1

3.1 / 4.1

5.3 Conclusies

3.1 | 4.1

6 Ontmantelen van botnets

Het slotstuk van een anti-botnet operatie zijn interventiemaatregelen, zoals C&C servers uit te (laten) schakelen of andere preventieve maatregelen te nemen. In dit hoofdstuk staan de relevante lessen uit Taurus voor het ontmantelen van botnets. Hierbij is voor het overgrote deel uitgegaan van het Taurusproject, maar waar relevant en niet conflicterend met het onderzoeksbelang zijn ook lessen over ontmanteling van botnets uit Tolling meegenomen. Achtereenvolgens worden hieronder beschreven de relevantie van het ontmantelen van botnets, de methode notice-and-takedown (NTD) en de conclusie.

6.1 Relevantie ontmantelen botnets

Het ontmantelen van botnets is ten eerste van belang voor het direct verminderen van de schadelijke activiteit van bepaalde botnets. Ten tweede gaat er een afschrikwekkende werking uit van een concrete interventie door de politie, zeker wanneer die in internationaal verband plaats vindt.12 Ten derde leidt het verminderen van het aantal C&C servers op Nederlandse bodem tot minder (noodzaak tot) internationale rechtshulpverzoeken aan Nederland. Onze 'infrastructuur' wordt namelijk een stukje schoner.

Dit kan echter alleen in samenwerking met private partijen, die immers een groot deel van deze infrastructuur beheren en beschikken over noodzakelijke kennis. Ook internationale samenwerking is gezien het internationale karakter van botnets en hun gebruikers noodzakelijk. In Taurus is daarom in beide samenwerkingsvormen voorzien.

Het uiteindelijk neer willen halen van botnets bleek een belangrijke reden voor diverse private partijen om deel te nemen aan Taurus. Meer nog dan *law enforcement agencies* zijn de meeste private partijen namelijk geïnteresseerd in de feitelijke uitschakeling van botnets, omdat dit het probleem van vandaag oplost. Het doen van langer durend onderzoek om uiteindelijk verdachten aan te houden heeft bij hen minder belangstelling.

12 Zie KLPD, Cybercrime – focus on high tech crime. Deelrapport criminaliteitsbeeld 2009, maart 2010, p. 81

Na bijna 750 botnets in kaart te hebben gebracht, leidde Taurus tot een grootschalige Notice & Takedown operatie in de herfst van 2010. Dit tijdstip was met name gekozen vanuit publicitair oogpunt, vlak voor het GOVCERT.NL symposium op 15 en 16 november 2010.

6.2

Voor de uitvoering van een grootschalige Notice & Takedown (NTD) vanuit de resultaten van een strafrechtelijk onderzoek, zoals in Taurus en Tolling, is hechte samenwerking nodig tussen het politiekorps en GOVCERT.NL. Vroege betrokkenheid van GOVCERT.NL zorgt voor een betere voorbereiding. Zo is in Taurus gewerkt met een beperkte proeflijst van uit de lucht te halen C&C servers. Deze proef was nuttig om de werkwijzen af te stemmen en te toetsen of de data voldoet voor een grootschalige NTD.

13 Operationeel Incident Response Team Overleg
14 Opstrust is een publiek-privaat netwerk van functionarissen die zich bezig houden met bestrijding van cyber crime. Dit netwerk is gebaseerd op vertrouwen op persoonsbasis.

Vrijwillig, maar met drukmiddelen

Het NTD proces is gebaseerd op vertrouwen én vrijwillige medewerking. Een CERT of ISP maakt een eigen afweging wel of niet iets te doen met een melding. Goed om te weten is, dat een takedown een kostenpost is voor een ISP. Hij krijgt er geen vergoeding voor.

De normale aanpak bij een NTD is de melding eerst via het netwerk van betrouwbare ISP's te doen en daarna pas naar minder betrouwbare partners. De kans dat er iets met de verstrekte informatie wordt gedaan, is dan namelijk groter. Publiciteit over take-downs kan een effectief middel zijn om de druk op andere ISP's te vergroten.

Hoe beter de data, des groter de bereidheid van ISP's om te handelen

Zoals gezegd, is NTD gebaseerd op vrijwillige medewerking van (o.a.) ISP's. Zij voeren een takedown bij sterke voorkeur alleen uit op nog actieve botnets (want de actie is een kostenpost, zonder dat daar inkomsten tegenover staan). De ervaring van GOVCERT.NL wijst uit, dat er meer kans is dat er iets gebeurt met de abuse melding, wanneer de informatie over het botnet actueel is, en de provider ook zelf met een MD5 sample van de activiteiten kan toetsen om wat voor soort activiteit het gaat.

De data van de Taurus NTD was echter wel actueel en voorzien van MD5 samples. Daar waren wel false positives, in de vorm van publieke channels waren niet gefilterd. ISP's negeerden deze meldingen, omdat zij deze wel konden herkennen als niet-zijnde een C&C server.

Meestal geen terugkoppeling over resultaten

Als GOVCERT.NL zijn partners heeft geïnformeerd, is meestal niet na te gaan wat er met de data gebeurt. In principe is het namelijk zo, dat de ISP zijn klant informeert en de voortgang bewaakt. Het is aan de ISP's om te besluiten of en welk actie ze nemen. GOVCERT.NL heeft ook geen autoriteit om iets af te dwingen. GOVCERT.NL verschaft ISP's wel de noodzakelijke informatie (b.v. IP-adres, MD5 samples). Vervolgens krijgt de klant van de ISP dan meestal eerst de gelegenheid om zelf te schonen. De ISP bewaakt dit proces, maar koppelt zelden terug. Op <20% van alle meldingen volgt terugkoppelingen, is de educated *guess* van GOVCERT.NL).

4.1

Om te weten of een ontmanteling via deze procedure daadwerkelijk effectief is, kunnen GOVCERT.NL en het en de politie dus een 'check' en een 'act' inbouwen in toekomstige gezamenlijke acties:

- 'check': het doen van een nieuwe meting op nog actieve botnets – liefst met schoning van false positives (KLPD-THTC of een andere politiekorps);
- 'act': herhalingsbericht met nog actieve C&C servers (GOVCERT.NL).

4.1

4.1

6.3 Conclusie

In dit hoofdstuk is met name beschreven hoe de methode NTD werkt bij het grootschalige ontmantelen van botnets. Deze methode werkt voor grootschalig neerhalen van C&C servers naar behoren, ook wanneer deze verspreid over de wereld draaien. Een kanttekening is dat de effectiviteit door het gebrek aan feedback lastig te volgen is. Een herhalingsactie verdient daarom altijd aanbeveling.

Wanneer één of meer partijen onbekend zijn met het NTD-proces of met het soort (opsporings-)onderzoek waaruit de botnetgegevens afkomstig zijn, verdient persoonlijke samenwerking tussen politie en GOVCERT.NL aanbeveling boven contact per mail of telefoon. Aangezien later in het proces veel meer partijen iets moeten doen, moeten de instructies zo helder mogelijk zijn. Dat kan alleen als de politie en GOVCERT.NL precies begrijpen wat moet worden gedaan en snel met elkaar kunnen schakelen om details af te stemmen.

De NTD is overigens niet de enige mogelijkheid om een botnet of botnets te ontmantelen, maar wel de meest efficiënte als het gaat om het uitschakelen van grote aantalen C&C servers. Alternatieven zijn het van binnenuit uitschakelen van een C&C server en/of het waarschuwen van gebruikers van besmette computers. Zie hierover ook het hoofdstuk Juridica.

Bijlage 1

Gebruikte documentatie

Bij het opstellen van het kennisdocument is gebruik gemaakt van de volgende schriftelijke bronnen:

Bevel Stelselmatige Inwinning (SI)

- Bevel Stelselmatige Inwinning 27/4 - 26/7 2010, Landelijk Parket;
- Aanvraag Verlenging bevel Stelselmatige Inwinning 21/7 - 24/10 2010, THTC;
- Verlenging bevel Stelselmatige Inwinning 21/7 - 24/10 2010, Landelijk Parket;
- Verlenging bevel Stelselmatige Inwinning 24/10 - 31/12 2010, Landelijk Parket.

Convenant

- Convenant informatie-uitwisseling aanpak botnets, 25 februari 2010,
- Toelichting convenant informatie-uitwisseling aanpak botnets, 25 februari 2010,

Nieuwsbrieven

- Nieuwsbrief 1, THTC, 22 september 2009;
- Nieuwsbrief 2, THTC, 13 oktober 2009;
- Nieuwsbrief 3, THTC, 21 december 2010.

Onderzoeksmonitoren

- Onderzoeksmonitor juni 2009, THTC;
- Onderzoeksmonitor september 2009, THTC;
- Onderzoeksmonitor januari 2010, THTC;
- Onderzoeksmonitor februari 2010, THTC;
- Onderzoeksmonitor maart 2010, THTC;
- Onderzoeksmonitor april 2010, THTC;
- Onderzoeksmonitor juni 2010, THTC;
- Onderzoeksmonitor augustus 2010, THTC.

Overig

- Verslag Eerste Expertmeeting, THTC, 30 september 2009;
- Verslag en opvolging meeting met 6.1 THTC, 2 april 2010;
- Request for operational data, THTC, 22 april 2010;
- USB-keys en uitleg Taurus-server, THTC, april 2010;
- Opzet projectplan Tolling, THTC, 21 september 2010;
- Cybercrime – focus on hightech crime. Deelrapport criminaliteitsbeeld 2009, KLPD maart 2010.

Processen-Verbaal

- Omschrijving georganiseerd verband, THTC, 26 april 2010;
- 3.1 | 4.1
- Start Nationaal Onderzoek, THTC, 13 september 2010;
- Command and control servers, THTC, 6 oktober 2010.

Projectplan Taurus

- Plan van aanpak Informatiegestuurde Aanpak van Botnets versie 1.2, THTC, 8 juni 2009;
- Aanvullend Projectplan Taurus, THTC, 4 maart 2010;
- Aanvullend projectplan Taurus, THTC, 8 juli 2010.

Bijlage 2

Interviews

Voor het opstellen van het kennisdocument zijn in totaal 16 personen in 15 interviews bevraagd.

Organisatie

- 6.1
- KLPD
- 3.1
- Landelijk Parket - Openbaar Ministerie
- 6.1

Interviewprotocol

Elk gesprek werd gevoerd door de senior onderzoeker en de onderzoeker, aan de hand van een interviewformulier. Dit formulier had als doel de volledigheid te borgen en volgde dan ook de onderwerpen van de evaluatie en de kennisdocumenten. Elk gesprek ging in op proces- en kennisaspecten en had de volgende structuur:

- Voorstelronde, uitleg doel en opzet van interviews.
- Start gesprek met rol van respondent (zo nodig ook uitleg over bedrijf / organisatie).
- Vervolgens naar bevindt van zaken in het gesprek de voorbereide onderwerpen langs laten komen. Proces en kennisdomeinen kunnen daarin door elkaar heenlopen. In de rapportage worden deze elementen uitgesplitst
- Afronding en afspraak over review verslag. De interviewverslagen volgen zoveel mogelijk de kopjes van de bovenstaande blokken voor verwerking in evaluatie- en kennisdocumenten.

Vrijwel alle interviews bestonden uit bijeenkomsten, op locatie van de respondent. Bij buitenlandse respondenten wordt een call opgezet. De onderzoeker is verantwoordelijk voor verslaglegging. Dit verslag is in alle gevallen ook getoetst door de respondent, voordat de inhoud ervan is gebruikt in evaluatie of kennisdocument. Waar nodig zijn later nog aanvullende vragen gesteld.

Bijlage 3

gebruikte afkortingen

BKA	Bundes Kriminal Ambt
BSI	Bundesambt für Sicherheit in Informationstechnik
C&C	Command & Control
CBP	College Bescherming Persoonsgegevens
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DNR	Divisie Nationale Recherche
DNS	Domain Name System
EGC	European Government CERTs
FBI	Federal Bureau of Investigation),
FPGA	Field Programmable Gate Arrays
FSB	Secret Service of Russia),
IP	Internet Protocol, Intellectual Property
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center.
ISP	Internet Service Provider
KLPD	Korps Landelijke Politiediensten
LP	Landelijk Parket
MD5	Message Digest Algorithm 5
PAC	Programma Aanpak Cybercrime
NFI	Nederlands Forensisch Instituut
NTD	Notice-and-Takedown
O-IRT-O	Operationeel Incident Response Team overleg
OM	Openbaar Ministerie
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OvJ	Officier van Justitie
P2P	Peer to peer
PoC	Proof of Concept
PPS	Publiek Private Samenwerking
PvA	Plan van Aanpak
SBU	Security Service of Ukraine
SI	Stelselmatige inwinning van informatie (126qa WvSv)

TDE	Team Digitale Expertise
TDI	Team Digitaal & Internet
THTC	Team High Tech Crime
Wpg	Wet Politiegegevens
Wsjg	Wet justitiële en strafvorderlijke gegevens
WvSr	Wetboek van Strafrecht
WvSv	Wetboek van Strafvordering
XML	Extensible Markup Language