Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Schedeldoekshaven 100
2511 EX Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
282560

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 15 oktober 2012
Onderwerp Wetgeving bestrijding cybercrime

Met deze brief doe ik mijn toezegging gestand uw Kamer een bericht te sturen over mijn inventarisatie van noodzakelijke, nieuwe strafrechtelijke opsporingsbevoegdheden op het internet[1].

Samenvatting

Deze brief bevat voorstellen om binnen de kaders van de rechtsstatelijkheid, proportionaliteit, subsidiariteit en eerbiediging van de persoonlijke levenssfeer van burgers, een aantal onderwerpen in wetgeving uit te werken om daarmee de bevoegdheden op het gebied van de opsporing en vervolging van cybercrime te versterken. Doel van deze nieuwe wetgeving is het juridisch kader voor de opsporing en vervolging van cybercrime meer toe te snijden op de door de diensten, die zijn belast met de opsporing en vervolging van cybercrime, gesignaleerde behoeften. Op grond van de praktijkervaringen en wensen, zoals die ook blijken uit de recente cybersecuritybeelden uit 2011 en 2012 en mijn brief aan uw Kamer van 23 december 2011 over het juridisch kader voor cybersecurity, betreft dit de volgende onderwerpen:

- Het op afstand binnendringen van geautomatiseerde werken (=computers) en het plaatsen van technische hulpmiddelen (waaronder software) ten behoeve van de opsporing van ernstige vormen van cybercrime;
- Het op afstand doorzoeken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, ongeacht de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen en met inachtneming van de afspraken en regels over de internationale rechtshulp;
- Het op afstand ontoegankelijk maken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, ongeacht de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen en met inachtneming van de afspraken en regels over de internationale rechtshulp.
- De strafbaarstelling van het helen van (digitale) gegevens.

De opbouw van deze brief is als volgt: als eerste wordt een aantal inleidende opmerkingen gemaakt (paragraaf 1), daarna worden de bovengenoemde

[1] Brief van 23 december 2011, o.a. over het juridisch kader voor cybersecurity, (TK, 2011-2012, 26643, nr. 220); antwoorden op vragen van lid Recourt (TK, 2011-2012, 1908); verslag van het AO “cybersecurity op 10 april 2012 (TK, 2011-2012, 26643, nr. 240).

onderwerpen nader uitgewerkt (paragraaf 2). Vervolgens wordt nader ingegaan op de strafvorderlijke waarborgen (paragraaf 3) en worden internationale ontwikkelingen geschetst (paragraaf 4). Tot slot geef ik aan welke vervolgstappen aan de orde zijn (paragraaf 5).

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

1. Inleidende opmerkingen

ICT toepassingen spelen een steeds grotere rol in het dagelijks leven. De actuele situatie is dat het aantal cybermisdrijven toeneemt en de capaciteit, kennis en ervaring binnen de strafrechtketen hiermee geen gelijke pas houdt. Onze mogelijkheden om er nationaal en internationaal iets tegen te doen nemen door het grensoverschrijdend karakter en de opkomst van zogenoemde cloud computing verder af. Verder blijkt dat de zelfregulatie van de industrie gebrekkig werkt en strafbare feiten die eigenlijk voorkomen zouden kunnen worden door betere en eerdere technische maatregelen vaak toch plaatsvinden.[2] Prangend is dat het zeer gecompliceerd is geworden om criminele activiteiten op het internet te traceren omdat het betrekkelijk eenvoudig voor criminelen is om te voorkomen dat digitale sporen kunnen worden gevolgd, bijvoorbeeld door het gebruik van software om gegevens te versleutelen en voor het wissen van het communicatiepad. De onderzoeken van het Team High Tech Crime van het KLPD (THTC) bevestigen dit. In het onderzoek naar kinderpornografie op het Tor-netwerk stelde het team vast dat door middel van het gebruik van dit netwerk het mogelijk is om kinderporno afbeeldingen op servers te bekijken, te downloaden of te uploaden, zonder dat de identiteit van de verdachte zichtbaar is. Verder werd er op diverse plaatsen, waaronder op de aangetroffen servers, gebruik gemaakt van versleuteling. De huidige versleuteltechnieken zijn zodanig ingewikkeld dat het ontsluiten met de huidige kennis vaak jaren in beslag zal nemen, ondanks het gebruik van veel computerkracht. In een ander onderzoek naar een groot botnet waarmee veel criminaliteit werd gepleegd, constateerde het THTC dat de eigenaar van het botnet met slechts enkele toetsaanslagen op zijn computer zijn gegevensbestanden simpel en in zeer korte tijd kon verplaatsen over de hele wereld, waardoor het vaststellen waar deze gegevens op servers stonden ernstig werd gehinderd dan wel onmogelijk was voor de opsporing. Ik ben van mening dat dit soort contramaatregelen van verdachten tegen de opsporing niet succesvol dienen te zijn. De gepleegde misdrijven dienen te worden opgespoord en daders vervolgd. De samenleving verwacht dit van de overheid.

Gegevens waarvan niet kan worden achterhaald waar op de wereld deze zijn vastgelegd

De politie en het OM signaleren dat zij in de praktijk nu behoefte hebben aan vergroting van de wettelijke mogelijkheden om te handelen, zodat de gewenste en afgesproken opsporings- en vervolgingsprestaties kunnen worden geleverd. Op dit moment probeert de politie de beperkte wettelijke mogelijkheden om opsporingshandelingen via het internet te verrichten te compenseren. Zo heeft de politie bijvoorbeeld de inhoud van servers op het hierboven al beschreven Tor netwerk met daarop opgeslagen afbeeldingen van ernstig seksueel misbruik van kinderen gekopieerd en daarna vernietigd dan wel ontoegankelijk gemaakt op de server. Op dat moment kon de exacte locatie van deze servers niet met zekerheid worden bepaald doordat het communicatiepad versluierd was. Het resultaat van

[2] Zie hiervoor het Cybersecuritybeeld 2012, toegezonden aan de Tweede Kamer op 6 juli 2012.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

de aanpak in deze zaak is dat de gekopieerde gegevens nu verder voor (internationaal) onderzoek kunnen worden gebruikt en toegang tot de bedoelde afbeeldingen via het internet niet meer mogelijk is via deze servers. In dit specifieke voorbeeld is door het OM en de politie een afweging gemaakt die in het voordeel van de bestrijding van kinderpornografie op internet is uitgevallen. Een dergelijke afweging zal ook in de toekomst gemaakt moeten worden bij de bestrijding van bijvoorbeeld botnets. Actualisering van wetgeving die een stevige basis voor politie en om geeft om haar noodzakelijk werk ten behoeve van de opsporing en vervolging op internet te verrichten op basis van dergelijke praktijkgevallen acht ik noodzakelijk.

Mobiel internetgebruik

De huidige strafvorderlijke bevoegdheden voor het bestrijden van cybercrime (artikelen 125i-125o van het Wetboek van Strafvordering) gaan in belangrijke mate uit van de situatie dat computers op een vaste plek staan en dat digitale gegevens op een enkele, individualiseerbare, computer zijn opgeslagen. Inmiddels is de digitale wereld sterk veranderd. De bevoegdheden zijn daardoor niet meer toereikend. In dit verband kan worden gewezen op de mogelijkheden van moderne mobiele computers, zoals smartphones en in toenemende mate tablets, en de manier waarop ze gebruikt worden. Deze nieuwe vormen van mobiele computers kunnen voortdurend verbonden zijn met het internet en kunnen gebruikt worden voor vele vormen van cybercrime. Daarnaast worden ze veelvuldig gebruikt door criminelen ten behoeve van hun gezamenlijke communicatie. Het versluieren van deze communicatie neemt steeds meer toe. Ook door het meer gebruiken van cloud computing zal het steeds moeilijker zijn voor de opsporing om te achterhalen waar gegevens van de desbetreffende smartphone of tablet op een bepaald moment opgeslagen zijn, terwijl het nog maar de vraag is hoe lang die gegevens daar opgeslagen zijn en daarmee traceerbaar blijven. Ik vind dat de bevoegdheden voor de bestrijding van cybercrime zodanig dienen te zijn vormgegeven dat deze hanteerbaar en effectief zijn in de huidige digitale wereld van mobiele apparatuur en cloud computing. Voor de mogelijkheden van digitale opsporing moet het in beginsel geen verschil maken waar een geautomatiseerd werk zich ten tijde van het verrichten van de wenselijke opsporingshandelingen bevindt. Volgens het internationale recht kunnen (digitale) onderzoekshandelingen op het grondgebied van een andere staat alleen via internationale rechtshulp worden verricht. Maar zoals uit het bovenstaande voorbeelden blijkt zal niet altijd kunnen worden vastgesteld waar de betreffende gegevens zich bevinden. Als dat het geval is, moeten politie en justitie onder de voorwaarden die hieronder in deze brief worden beschreven, verder kunnen opsporen.

2. Uitwerking van de bovengenoemde wetgevingsvoornemens

Hieronder worden de wetgevingsvoornemens die ik hierboven heb aangekondigd verder toegelicht.

2.1. Het op afstand binnendringen van geautomatiseerde werken (=computers) en het plaatsen van technische hulpmiddelen (waaronder software) ten behoeve van de opsporing van ernstige vormen van cybercrime.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

In paragraaf 1 is de ontwikkeling weergegeven naar meer mobiel internet gebruik. Ook het steeds meer versleutelen van de computergegevens is daar aan de orde gesteld. Politie en OM geven aan dat er allerlei vormen van criminaliteit zijn die zich aan het zicht van politie en OM onttrekken omdat zij niet de bevoegdheid hebben om een computer te mogen binnendringen.
Artikel 125i Sv biedt binnen zekere kaders de bevoegdheid tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd. In het belang van het onderzoek kunnen deze gegevens worden vastgelegd. Uit de parlementaire geschiedenis kan worden afgeleid dat niet toegelaten is om een geautomatiseerd werk *op afstand* binnen te dringen ten behoeve van de opsporing van ernstige vormen van cybercrime.[3] Hierbij kan zowel worden gedacht aan het op afstand binnendringen ten behoeve van het aftappen van vertrouwelijke communicatie als aan het binnendringen ten behoeve van de doorzoeking van een geautomatiseerd werk[4]. Om ten behoeve van de opsporing van ernstige vormen van cybercrime toegang te kunnen krijgen tot deze gegevens, is het nodig dat heimelijk software kan worden geïnstalleerd met behulp waarvan de versleuteling van de gegevens ongedaan kan worden gemaakt of omzeild kan worden.[5]

Mede in het licht van technologische ontwikkelingen dient een wettelijke bevoegdheid te worden gecreëerd om op afstand een geautomatiseerd werk binnen te dringen, met het oog op de hierboven weergegeven doelen. De gewijzigde omstandigheden rechtvaardigen dat een specifieke bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk ten behoeve van de opsporing van ernstige vormen van cybercrime wordt opgenomen in het Wetboek van Strafvordering.

2.2. Het op afstand doorzoeken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, in het geval de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen niet kan worden bepaald, met inachtneming van de afspraken en regels over de internationale rechtshulp.

In paragraaf 1 heb ik het voorbeeld gegeven van een botnet waarbij de crimineel in staat was om zeer snel zijn gegevens over de wereld te verplaatsen. Dit is steeds meer de huidige

[3] De inlichtingen- en veiligheidsdiensten beschikken op grond van artikel 24 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 al over een dergelijke bevoegdheid. In de parlementaire geschiedenis van die wet is expliciet aan de orde gesteld dat opsporingsdiensten niet de bevoegdheid hebben een geautomatiseerd werk binnen te dringen. Als reden hiervoor is gegeven dat dit niet noodzakelijk zou zijn voor de opsporing.

[4] Deze wettelijke bevoegdheid is in Frankrijk vrij recent geïntroduceerd (Loi d'orientation et de programmation pour la performance de la sécurité intérieure). In België ligt een wetsvoorstel voor waarin ruime bevoegdheden worden gecreëerd ten aanzien van het plaatsen van technische hulpmiddelen en het doel waarvoor zij aangewend mogen worden.

[5] In dit verband moet worden opgemerkt dat thans een wetenschappelijk onderzoek wordt verricht naar de juridische basis om een bevel tot het ontsleutelen van gegevens, op basis van artikel 125k Sv, ook aan de verdachte zelf te richten. Hiervoor kan worden verwezen naar de brief aan uw Kamer van 27 januari 2012 (Kamerstukken II 2011/12, 31 015, nr. 77). De bevindingen van dit onderzoek zullen binnenkort beschikbaar komen en worden betrokken bij de verdere besluitvorming over de aanpassing van het wettelijke instrumentarium voor de bestrijding van ernstige vormen van cybercrime.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

praktijk. Criminelen weten dat de politie probeert om toegang te krijgen tot hun netwerken en gegevens en treffen daartegen maatregelen. Doorgaans worden de desbetreffende gegevens snel over het internet (wereldwijd) verplaatst c.q. de paden daartoe aangepast. Ook worden door criminele groeperingen dikwijls maatregelen getroffen om vast te stellen of derden, waaronder de politie, proberen zich toegang te verschaffen tot hun bestanden. Indien zij dergelijke signalen opvangen of vermoeden verplaatsen zij hun bestanden zo snel mogelijk en schuwen niet om indringers met digitale middelen te bestrijden.
Deze technische ontwikkelingen leiden ertoe dat de locatie van opgeslagen gegevens moeilijk is vast te stellen en vaak wijzigt. Werden de gegevens voorheen doorgaans op de eigen computer of op een afzonderlijke gegevensdrager opgeslagen, inmiddels worden gegevens met behulp van internet eenvoudig op een server in het buitenland of in de cloud worden opgeslagen.
Uitgangspunt is dat strafvorderlijke bevoegdheden alleen op het eigen grondgebied kunnen worden uitgeoefend. Voor het uitvoeren van opsporingshandelingen op het grondgebied van een andere staat is een rechtshulpverzoek vereist. Het omgekeerde geldt evenzeer: als een vreemde staat opsporingshandelingen op het grondgebied van Nederland verricht wil zien is een rechtshulpverzoek vereist (artikel 552h Sv). Echter, de tijd die met een rechtshulpverzoek verstrijkt werkt in het geval van cybercrime vaak in het nadeel van de opsporing en beperkt de effectiviteit van rechtshulp.
In het Cybercrimeverdrag van de Raad van Europa kent een bepaling over het op afstand verschaffen van toegang tot computergegevens ongeacht waar die gegevens zijn opgeslagen (artikel 32). Deze toegang is beperkt tot openbaar toegankelijke gegevens en tot andere gegevens op voorwaarde van instemming van de rechthebbende. Het Cybercrimeverdrag bevat geen bepalingen over het zonder toestemming van de rechthebbende vergaren van gegevens die niet openbaar toegankelijk zijn, zodat daarvoor een rechtshulpverzoek noodzakelijk is. Maar bij het op afstand doorzoeken van computers is het in de praktijk zoals hierboven al is beargumenteerd, niet altijd goed te bepalen waar de gegevens zich bevinden. Een verzoek om rechtshulp is dan niet mogelijk. Het is vanuit het oogpunt van een doelmatige opsporing van essentieel belang dat gegevens kunnen worden verkregen ongeacht de plaats waar zij zijn opgeslagen. Daarom hebben de politie en het OM aangedrongen op een wettelijke regeling ter zake.
Voor de wettelijke regeling die ik op het oog heb, hanteer ik de volgende uitgangspunten. Indien er wetenschap is van de locatie van de gegevens, en deze zich op een server in het buitenland bevinden, dan is een rechtshulpverzoek aangewezen. Indien er geen wetenschap is van de locatie van de opgeslagen gegevens, dan dienen zij met het oog op de bewijsvergaring te kunnen worden doorzocht en overgenomen. Ook in het Belgische Wetboek van Strafvordering is geregeld dat bij het doorzoeken van een geautomatiseerd werk gegevens kunnen worden overgenomen. Wanneer blijkt dat de gegevens zich niet op het grondgebied van België bevinden dan worden de gegevens alleen gekopieerd en wordt de betrokken staat geïnformeerd (artikel 88ter).

2.3. Het op afstand ontoegankelijk maken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, in het geval de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen niet kan worden bepaald, met inachtneming van de afspraken en regels over de internationale rechtshulp.

Een bijzonder aspect betreft de mogelijkheid van het ontoegankelijk maken van gegevens die worden aangetroffen bij het op afstand doorzoeken van een

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

geautomatiseerd werk. In Nederland bestaat thans de mogelijkheid dat, wanneer een plaats is betreden ter vastlegging van gegevens die daar op een gegevensdrager zijn vastgesteld, en het gaat om gegevens met betrekking tot welke of met behulp waarvan het strafbaar feit is begaan (bijvoorbeeld kinderporno), de gegevens ontoegankelijk worden gemaakt ter beëindiging van het strafbaar feit (artikel 125o Sv). In aansluiting daarbij is het wenselijk om bij introductie van een bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk en het op afstand doorzoeken van gegevens, ook een bevoegdheid te scheppen om dergelijke gegevens ontoegankelijk te maken. Het kan immers voorkomen dat bij het op afstand doorzoeken van een computer bijvoorbeeld kinderporno wordt aangetroffen. Dit was aan de orde bij het eerdergenoemd onderzoek dat het THTC deed naar kinderpornografische beelden op servers in het TOR-netwerk, waar de politie zeer schadelijk kinderpornografisch materiaal aantrof dat in versleutelde vorm was opgeslagen op een server. Bij afwezigheid van kennis van de locatie van opslag van de gegevens is rechtshulp zoeken niet mogelijk. Niemand kan dan worden aangesproken, terwijl het strafbare feit voortduurt. De ernst van de strafbare feiten kan vereisen dat de gegevens onverwijld ontoegankelijk worden gemaakt. Dit kan met zich brengen dat de gegevens worden verwijderd. Daarom acht ik het wenselijk dat een wettelijke bevoegdheid wordt gecreëerd tot het ontoegankelijk maken of verwijderen van de gegevens die worden aangetroffen bij het op afstand doorzoeken van een geautomatiseerd werk, naar het model van de regeling van artikel 125o van het Wetboek van Strafvordering. Ook hier geldt dat wanneer wetenschap bestaat van de locatie van de gegevens, een rechtshulpverzoek aan de bevoegde autoriteiten van de desbetreffende staat moet worden gericht.

2.4. Strafbaarstelling van het helen van (digitale) gegevens

Er worden op internet feiten gepleegd waarbij gegevens worden verkregen via hacking of andere wijze, die interessant zijn voor derden om te kunnen gebruiken voor criminaliteit. Voorbeelden hiervan zijn persoonsgegevens uit databases die gekraakt zijn en daarna gebruikt kunnen worden om bijvoorbeeld goederen te kopen op het internet bij marktplaats e.d. Ook worden creditcardgegevens die via phishing worden verkregen, aangeboden op het internet en verkocht. Hoewel in dit laatste geval het gebruik van deze gegevens om creditcards te maken al strafbaar is gesteld, is het voorhanden hebben, het overdragen en het kopen van deze gegevens zelf niet strafbaar. Dit maakt het voor de opsporing lastig. Het wachten tot dat de gegevens daadwerkelijk worden gebruikt voor criminaliteit, betekent dat er niet opgetreden kan worden om misdrijven te voorkomen. Dat is zeker niet vertrouwenwekkend naar de burger en in feite een slecht signaal omdat deze vorm van heling in digitale zin wel zou mogen. Het verhandelen of verkopen van dergelijke gegevens heeft zich ontwikkeld tot een zich zelfstaande vorm van criminaliteit.
Dat heling van dit soort gegevens thans niet strafbaar is, houdt verband met het feit dat computergegevens op grond van de jurisprudentie slechts in bepaalde omstandigheden als een goed in de zin van de artikelen 310 en 416 van het Wetboek van Strafrecht (Sr) worden aangemerkt. Dit is aan de orde als gegevens buiten de beschikkingsmacht van de rechthebbende zijn gebracht en in het economisch verkeer waarde vertegenwoordigen. Hieruit vloeit voort dat het zonder toestemming van de rechthebbende kopiëren van diens gegevens en het vervolgens gebruiken of verhandelen van die gegevens als zodanig niet strafbaar is omdat de rechthebbende de beschikkingsmacht over die gegevens behoudt. Ik ben van mening dat het voor de betrokken slachtoffers onaanvaardbaar is dat de

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560

bestaande wetgeving in de digitale wereld tot ongewenste lacunes leidt en acht het wenselijk op dit punt te komen tot aanvullende strafbaarstellingen.

3. Strafvorderlijke waarborgen

De in de paragrafen 2.1 t/m 2.3 beschreven bevoegdheden moeten met strikte waarborgen worden omgeven. De bevoegdheid tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd, op grond van artikel 125i Sv, komt, afhankelijk van de plaats waar wordt gezocht en de ernst van de verdenking, zowel aan de rechter-commissaris, de officier van justitie, de hulpofficier van justitie als de opsporingsambtenaar toe. Bij verschillende andere bevoegdheden is specifiek bepaald dat de rechter-commissaris of de officier van justitie bevoegd is (bijvoorbeeld de artikelen 125la, 125n, derde lid en 125o, eerste lid Sv). Maar gezien de mate van ingrijpendheid van de wettelijke bevoegdheden tot het op afstand binnendringen van geautomatiseerde werken en het plaatsen van technische hulpmiddelen ten behoeve van de opsporing van ernstige vormen van cybercrime, vooral gelet op de inbreuk die daardoor wordt gemaakt op het recht op eerbiediging van de persoonlijke levenssfeer van personen, zal steeds een voorafgaande machtiging van de rechter-commissaris dienen te zijn verkregen. Ook zal de bevoegdheid alleen kunnen worden uitgeoefend bij verdenking van strafbare feiten van een zekere ernst, bijvoorbeeld misdrijven waarvoor voorlopige hechtenis voorzien is of waarop een maximale gevangenisstraf van vier jaar of meer is gesteld.
Verder geldt uiteraard ook bij deze bevoegdheden de algemene eis dat van de uitoefening daarvan proces-verbaal moet worden opgemaakt. Daarnaast zullen alle bij de uitoefening van deze bevoegdheden verrichte handelingen automatisch worden gelogd en bewaard en daardoor achteraf altijd raadpleegbaar en controleerbaar zijn.

4. Internationale ontwikkelingen

Al eerder heb ik u bericht dat Nederland in internationaal verband stevig meewerkt aan het verder ontwikkelen van het internationale kader, vooral in het verband van de Raad van Europa. Nederland is zowel lid van de Convention Committee (waar alle verdragsluitende partijen lid van zijn) als van het Bureau (een gekozen orgaan binnen de Convention Committee) die aan het Cybercrimeverdrag van de Raad van Europa gekoppeld zijn. In dat kader dragen wij bij aan het actief werven van nieuwe leden van dit verdrag. Inmiddels zijn 33 landen tot het verdrag toegetreden (waarvan ook 17 geratificeerd hebben), waaronder 2 niet-Europese landen (de Verenigde Staten en Japan)[6]. Mede op instigatie van Nederland is sinds 2010 een discussie aangezwengeld over de reikwijdte van artikel 32 van het verdrag dat hierboven al aan de orde kwam. Ik acht het van groot belang dat enigerlei bevoegdheid tot grensoverschrijdende opsporing internationaal geborgd wordt. Dit is een traject dat vele jaren zal kosten. Nederland zal daar voortdurend de hand aan de pols houden. Ik kies ervoor om in Nederland zelf de verbeteringen voor de bestrijding van cybercrime al in gang te zetten.

5. Vervolgstappen

[6] Nederland heeft het Cybercrimeverdrag in 2006 geratificeerd.

De komende maanden zullen worden gebruikt om samen met de politie, het openbaar ministerie en andere relevante betrokkenen de nadere uitwerking ter hand te nemen die nodig is om op basis daarvan een conceptwetsvoorstel voor te bereiden. Ik ben ervan overtuigd dat deze inhaalslag nodig is om de opsporing en vervolging van cybercrime te versterken.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DGRR/DRC/C&V

Datum
15 oktober 2012

Ons kenmerk
282560