Nr. 001

Ministerie van Veiligheid en Justitie

De Minister

Sector straf- en sanctierecht
**Contactpersoon**
10.2.E

**Datum**
...april 2013

**Ons kenmerk**
volgt

**Dossiernummer**
volgt

# nota

Conceptwetsvoorstel versterking bestrijding computercriminaliteit

**Algemene leiding**

| Minister | Staatssecretaris | SG |
|---|---|---|
| Datum/eindparaaf | Datum/paraaf | Datum/paraaf |

**Door tussenkomst van**

| DWJZ | Hoofd sector straf- en sanctierecht |
|---|---|
| Datum/paraaf | Datum/paraaf |

**Van**
10.2.E
Datum/paraaf

**Visie vooraf**

| Directeur DRC | 10.2.E |
|---|---|
| Datum/paraaf | Datum/paraaf |

**Gevraagde beslissing:** Instemming met het in consultatie geven van het conceptwetsvoorstel versterking bestrijding computercriminaliteit.

**Samenvatting:** Het conceptwetsvoorstel bevat de volgende onderdelen:
a) Het op afstand heimelijk binnentreden van computers;
b) Het decryptiebevel aan de verdachte;
c) Aanpassing van de procedure voor het ontoegankelijk maken van gegevens;
d) Strafbaarstelling van het wederrechtelijk kopiëren van gegevens en van "heling" van gegevens.

## I. Achtergrond

Bij brief van 15 oktober 2012 heeft u de Tweede Kamer geïnformeerd over uw voornemen om een aantal onderwerpen in wetgeving uit te werken om daarmee de bevoegdheden op het gebied van de opsporing en vervolging van cybercrime te versterken. In de brief is aangegeven dat mede in het licht van de technologische ontwikkelingen een bevoegdheid dient te worden gecreëerd om op afstand een geautomatiseerd werk binnen te dringen, met het oog op de opsporing van ernstige vormen van cybercrime (ook wel aangeduid als het 'on line hacken van computers'). De gegevens kunnen zich op een server in het buitenland bevinden. In voorkomende gevallen moeten dergelijke gegevens ontoegankelijk gemaakt kunnen worden. Toegezegd is dat de komende maanden de nadere uitwerking ter hand zou worden genomen ter voorbereiding van een conceptwetsvoorstel.

Bij brief van 28 november 2012 heeft u de Tweede Kamer vervolgens geïnformeerd over het decryptiebevel. In de brief wordt verwezen naar de ervaringen in de strafzaak tegen Robert M., waarbij de verdachte afbeeldingen van kinderpornografie in zijn computer had versleuteld. In het Wetboek van Strafvordering zou een bevoegdheid moeten worden opgenomen tot het geven van een bevel aan een verdachte tot het verschaffen van toegang tot versleutelde elektronische gegevens en het toegankelijk maken van die gegevens (decryptiebevel aan de verdachte). Vanwege de inbreuk op het beginsel van nemo tenetur wordt de uitoefening beperkt tot de vervaardiging, de verspreiding en het bezit van kinderpornografie (art. 240b Sr) en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens. Er zullen zeer strikte waarborgen gelden voor de uitoefening van deze bevoegdheid. Het opzettelijk niet voldoen aan het decryptiebevel wordt afzonderlijk strafbaar gesteld. De keuze voor een specifieke strafbedreiging zal in het wetsvoorstel nader worden beargumenteerd. In het AO van 6 december over Informatie- en communicatietechnologie (ICT) is door u gemeld dat het de bedoeling is om de conceptwetgeving in het eerste kwartaal van 2013 in consultatie te geven (Kamerstukken II 2012/13, 26 643, nr. 265, blz. 16).

In 2010 reeds is aan u een conceptwetsvoorstel voorgelegd ter versterking van de bestrijding van computercriminaliteit. Dat wetsvoorstel voorzag eveneens in de aanpassing van de procedure voor de ontoegankelijkmaking van gegevens en de strafbaarstelling van heling van gegevens. Naar aanleiding van de consultatie is dit conceptwetsvoorstel destijds, in overleg met u en de staatssecretaris, niet verder in procedure gebracht. Inmiddels heeft u besloten dat deze twee onderwerpen toch wettelijke regeling behoeven; daarom zijn zij opnieuw in dit conceptwetsvoorstel betrokken. Dit wordt hieronder nader toegelicht.

## II. Toelichting

a. Onderzoek in een geautomatiseerd werk

Voorgesteld wordt dat bepaalde opsporingsambtenaren een geautomatiseerd werk op afstand heimelijk kunnen binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van strafbare feiten. Die doelen zijn in het wetsvoorstel beschreven en betreffen het volgende:

a. Het vaststellen van de aanwezigheid van gegevens of het identificeren van het geautomatiseerde werk of de gebruiker ('virtuele plaatsopneming');
b. Het overnemen van gegevens (afbeeldingen van kinderpornografie of een opgeslagen e-mailbericht);

c. De ontoegankelijkmaking van gegevens (afsluiten van botnets);
d. Het aftappen van telecommunicatie (de telefoontap) en het opnemen van vertrouwelijke communicatie (de richtmicrofoon);
e. De stelselmatige observatie.

Dit geheel aan handelingen (binnendringen en uitvoering van bepaalde opsporingshandelingen) wordt in het wetsvoorstel aangeduid als: onderzoek in een geautomatiseerd werk. Deze bevoegdheid is nodig vanwege de ontwikkelingen op het gebied van de communicatietechnologie. Computergegevens kunnen eenvoudig worden versleuteld waardoor deze voor politie en justitie onleesbaar zijn. Versleutelingsprogramma's worden op internet aangeboden. Dit betreft overigens niet alleen de doorgewinterde criminelen maar ook de communicatie van de 'Blackberry' en de 'Iphone' wordt door de fabrikanten standaard versleuteld. Daardoor wordt het tappen steeds lastiger, de enige oplossing is te tappen voordat de gegevens worden versleuteld en verzonden of nadat de gegevens zijn ontvangen en ontsleuteld. Aldus verschuift het focus van het tappen via de aanbieder van de communicatiedienst (KPN, Vodafone) naar het tappen op het apparaat (de smartphone). Dit is een verstrekkende ontwikkeling. Daarnaast vormen Clouddiensten, waarbij de gegevens op verschillende servers in de wereld worden opgeslagen om de kosten van opslag te drukken, een uitdaging voor de opsporing omdat niet bekend is waar de gegevens feitelijk zijn opgeslagen en aanbieders niet kunnen worden aangesproken op hun strafvorderlijke verplichtingen.

Er gelden strikte voorwaarden voor het onderzoek in een geautomatiseerd werk;
1. De inzet is beperkt tot ernstige strafbare feiten die een ernstige schending van de rechtsorde vormen;
2. Een bevel kan uitsluitend worden gegeven als het belang van het opsporingsonderzoek dat dringend vordert;
2. De uitvoering is voorbehouden aan bepaald aangewezen opsporingsambtenaren binnen de politie;
3. Er is een machtiging nodig van de rechter-commissaris;
4. De voorgenomen inzet wordt getoetst door de Centrale Toetsingscommissie (CTC) van het openbaar ministerie;
5. Er moet gebruikt worden gemaakt van een technisch hulpmiddel (software) die aan bepaalde eisen voldoet. De eisen worden uitgewerkt in het besluit technische hulpmiddelen strafvordering;
6. Er worden gegevens gelogd over de uitvoering van de bevoegdheid.

De gegevens kunnen op een server zijn opgeslagen die zich in een andere staat bevindt. Op grond van het Cybercrimeverdrag van de Raad van Europa, dat door Nederland is geratificeerd, is grensoverschrijdend optreden slechts in zeer beperkte gevallen mogelijk. Het is ook vanuit politiek oogpunt van belang binnen de kaders van het volkenrecht te blijven. In de memorie van toelichting wordt aangegeven dat wanneer niet bekend is waar de gegevens zijn opgeslagen, zelfstandig kan worden opgetreden. Dit geldt voor vrijwel alle gegevens die in de Cloud zijn opgeslagen. De gegevens kunnen worden vastgelegd of ontoegankelijk gemaakt, ongeacht de locatie waar de gegevens zich bevinden (blz. 34). Als de plaats van opslag wel bekend is, is zelfstandig optreden van de belanghebbende staat overigens bij voorbaat evenmin uitgesloten. Dit hangt af van de omstandigheden van het geval. Tijdens de voorbereiding van het wetsvoorstel hebben de vertegenwoordigers van politie en OM aangegeven met deze lijn goed uit de voeten te kunnen.

In het AO van 6 december 2012 hebben enkele fracties zich kritisch getoond over deze bevoegdheid (SP, CDA, D66, PVV). Daarbij gaat het om de verhouding tussen het middel en het doel (proportionaliteit van de maatregel), de inbreuk op de privacy en de internationale component.

In het AO van 6 december is door u toegezegd dat de wettelijke regeling van het onderzoek in een geautomatiseerd werk samen met een privacy impact assessment (PIA) in consultatie zou worden gegeven (Kamerstukken II 2012/13, 26643, nr. 265, blz. 21). De PIA is thans evenwel nog niet gereed; deze wordt tijdens de consultatie voltooid zodat het wetsvoorstel en de PIA tezamen aan de Raad van State kunnen worden gezonden. Tijdens de consultatie zal tevens worden nagegaan in hoeverre de rechterlijke macht, in het bijzonder de rechters-commissarissen en officieren van justitie, adequaat is opgeleid om uitvoering te geven aan de voorgestelde bevoegdheid.

De financiële paragraaf (paragraaf 6) is evenmin voltooid. Deze wordt afgerond tijdens de consultatie, in overleg met politie en openbaar ministerie.

b. Het decryptiebevel aan de verdachte

De voorgestelde regeling betreft de uitwerking van de bevindingen van het onderzoek van het TILT van de Universiteit Tilburg (prof. E.J. Koops). Dit onderzoek was ingegeven door de spanning met het beginsel van nemo tenetur (verdachte kan niet worden verplicht jegens zichzelf te getuigen) dat door artikel 6 EVRM wordt beschermd. Ook andere EU-lidstaten kennen de mogelijkheid van een decryptiebevel aan de verdachte (het VK en Frankrijk). De uitgangspunten voor de wettelijke regeling zijn neergelegd in de eerdergenoemde brief aan de Tweede Kamer van 28 november 2012. Deze uitgangspunten zijn als volgt:

1. Het decryptiebevel aan de verdachte is uitsluitend mogelijk bij verdenking van met maken van een beroep of gewoonte van het bezit en de verspreiding van kinderpornografie (art. 240b, tweede lid, Sr) en het plegen van terroristische misdrijven (art. 83 Sr). Voor een adequate bestrijding van deze strafbare feiten is het van groot belang dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens. Dit is ook in het belang van de veelal minderjarige slachtoffers;
2. Een bevel kan uitsluitend worden gegeven als het belang van het opsporingsonderzoek dat dringend vordert;
3. Het bevel zal uitsluitend gegeven kunnen worden door de officier van justitie, na schriftelijke machtiging van de rechter-commissaris.
4. De verdachte wordt vooraf gehoord, hij kan zich daarbij door een raadsman laten bijstaan;
5. Het opzettelijk niet voldoen aan een decryptiebevel wordt strafbaar gesteld met een gevangenisstraf van ten hoogste drie jaar en een boete van de vierde categorie.

In uw eerdergenoemde brief van 28 november is toegezegd dat in het wetsvoorstel een evaluatie- en horizonbepaling zou worden opgenomen voor de regeling van het decryptiebevel. Hiervan is vooralsnog afgezien, vanwege het risico dat aangedrongen wordt op verbreding van de evaluatie en de horizonbepaling voor het hele wetsvoorstel. Voorstel is om deze bepalingen achter de hand te houden; desgewenst kan dit in een later stadium (nota n.a.v. verslag of tijdens plenair debat) worden toegevoegd.

Naar verwachting staat de Tweede Kamer overwegend positief ten opzichte van het decryptiebevel aan de verdachte. Het openbaar ministerie en de politie zijn kritisch; zij betwijfelen of het decryptiebevel in de praktijk toepasbaar is (bewijsproblemen) en geven de voorkeur aan een wettelijke regeling van het onderzoek in een geautomatiseerd werk zodat versleutelde gegevens daadwerkelijk beschikbaar komen voor de opsporing.

c. Aanpassing van de procedure tot de ontoegankelijkmaking van gegevens

Het Wetboek van Strafrecht bevat een specifieke regeling voor het verwijderen van gegevens van het internet (art. 54a Sr). Dit wordt aangeduid als de ontoegankelijkmaking van gegevens. De huidige regeling omvat zowel een vervolgingsuitsluitingsgrond als een bevelsbevoegdheid van de officier van justitie. Deze combinatie blijkt de toepassing van de bevoegdheid in de praktijk te belemmeren. Daarom wordt voorgesteld de huidige regeling te splitsen in een strafrechtelijke bevoegdheid te bevelen gegevens ontoegankelijk te maken en een strafvorderlijke strafuitsluitingsgrond. Uitgangspunt blijft dat verwijdering zoveel mogelijk plaatsvindt op basis van de vrijwillige NTD-gedragscode.

Tijdens de eerdere consultatie is veel kritiek geleverd op het aanvankelijke voorstel tot schrapping van het vereiste van de machtiging van de rechter-commissaris voor de ontoegankelijkmaking van gegevens. De gedachte was dat de overheid censuur op het internet zou willen gaan uitoefenen. Ook de staatssecretaris heeft zich destijds als lid van de Tweede Kamer kritisch uitgelaten over de schrapping van het vereiste van de machtiging van de rechter-commissaris. Naar aanleiding van deze kritiek wordt thans voorgesteld deze machtiging te handhaven. Een rechter-commissaris moet bij uitstek in staat worden geacht in de gevallen, waarin de NTD-gedragscode geen soelaas biedt, een onpartijdige en zorgvuldige afweging te maken tussen de verschillende belangen. Dit is te meer van belang omdat hierbij ook de vrijheid van meningsuiting in het geding kan zijn.

Als de aanbieder niet voldoet aan de vordering ontoegankelijkmaking, kan hij worden vervolgd voor het niet voldoen aan een ambtelijk bevel (artikel 184 Sr) of, in voorkomende gevallen, voor het begaan van het achterliggende strafbaar feit (bijv. het verspreiden van afbeeldingen van kinderpornografie).

d. Strafbaarstelling van het wederrechtelijk overnemen en helen van gegevens

Dit betreft de strafbaarstelling van ‘diefstal’ en ‘heling’ van gegevens. De afgelopen jaren zijn gevallen in de publiciteit gekomen waarin gegevens uit een computer, bijvoorbeeld een e-mailbox, werden gekopieerd en op het internet geplaatst. Doorgaans kan de hacker worden vervolgd op grond van computervredebreuk (artikel 138a Sr) maar de “heler” van de gegevens gaat vrijuit.

Door aan artikel 139c Sr (aftappen van gegevens die worden overgedragen door middel van telecommunicatie of een geautomatiseerd werk) het “overnemen” van (niet openbare) gegevens toe te voegen, is ook degene strafbaar die rechtmatig toegang heeft tot computergegevens van een ander (bijv. een secretaresse) en de gegevens vervolgens wederrechtelijk overneemt. Degene die over wederrechtelijk overgenomen gegevens beschikt of deze aan een ander bekend maakt, wordt strafbaar door artikel 139e Sr (beschikken over/bekend maken van

afgetapte gegevens) aan te vullen met beschikken over/bekend maken van overgenomen gegevens. Aldus is ook "heling" van deze gegevens strafbaar.

De strafbaarstelling van diefstal en heling van gegevens zou kunnen worden uitgelegd als een poging van de overheid om journalisten en klokkenluiders aan te pakken (verg. de WikiLeaks-affaire). Om hieraan tegemoet te komen wordt voorgesteld een wettelijke uitzondering op te nemen voor personen die te goeder trouw hebben kunnen aannemen dat het algemeen belang bekendmaking van door misdrijf verkregen gegevens vereiste. De beoordeling of aan deze uitzondering is voldaan, is aan de rechter. Zo lang een journalist te goeder trouw heeft kunnen aannemen dat bekendmaking in het algemeen belang was vereist, is deze niet strafbaar. Overigens heeft de Hoge Raad onlangs in de zaak tegen de journalist Carlo Stegeman van SBS6, die het terrein van de luchthaven Schiphol was binnengedrongen, overwogen dat journalisten slechts onder bijzondere omstandigheden zijn ontslagen van hun plicht zich aan de strafwet te houden. In navolging van het EHRM heeft de Hoge Raad erkend dat het recht op vrije meningsuiting in de weg kan staan aan strafvervolging.

## III. De verhouding met de actualiteit

De afgelopen week is er veel aandacht geweest voor de zogenaamde DDoS-aanvallen (Distributed Denial of Service) op servers en websites van financiële instellingen. Het wetsvoorstel voorziet niet in strafbaarstelling; de DDoS-aanval is reeds strafbaar op grond van de artikelen 138ab (vier jaar gevangenisstraf), 138b (een jaar gevangenisstraf) en 161 sexies/septies Sr (één jaar tot vijftien jaar gevangenisstraf). Op deze artikelen heeft het openbaar ministerie reeds veroordelingen gekregen.
Ook is in de media aandacht besteed aan het aanbieden van materiaal voor het plegen van DDoS-aanvallen (Trouw 11/4). Het voorhanden hebben van hacktools is eveneens reeds strafbaar op grond van de artikelen 139d (één jaar gevangenisstraf) en 161 sexies Sr. Op deze artikelen heeft het openbaar ministerie eveneens reeds veroordelingen gekregen.

Het wetsvoorstel vereenvoudigt de beëindiging van DDoS-aanvallen, omdat het voorziet in de mogelijkheid van het binnendringen van de servers van waaruit de gegevens worden verstuurd, zodat deze kunnen worden afgesloten voor degene die deze gebruikt voor de DDoS-aanval (par. 2.3, onder punt 3).

## IV. Afstemming en consultatie

De inhoud van het conceptwetsvoorstel is afgestemd met DGRR/DRC, het openbaar ministerie (de landelijk officier van justitie computercriminaliteit) en de politie (Team High Tech Crime). Voorgesteld wordt het wetsvoorstel voor advies voor te leggen aan het College bescherming persoonsgegevens, het College van procureurs-generaal, de Korpschef van de Nationale Politie, de Nederlandse Orde van Advocaten, de Raad voor de Rechtspraak, de Nederlandse Vereniging voor Rechtspraak en de stichting Bits of Freedom (conceptbrieven bijgevoegd). Daarnaast zal het op het internet worden geplaatst, met het oog op openbare consultatie.

++

# Nr. 003

Ministerie van Veiligheid en Justitie

Minister

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

**Contactpersoon**
10.2.E

10.2.E

nota

Wetsvoorstel computercriminaliteit III aan de CBVJ

**Datum**
5 december 2013

**Ons kenmerk**
volgt

**Dossiernummer**
volgt

| **Algemene leiding** | |
|---|---|
| Minister | SG |
| Datum/eindparaaf | Datum/paraaf |

| **Door tussenkomst van** | |
|---|---|
| DW | Hoofd sector straf- en sanctierecht |
| Datum/paraaf | Datum/paraaf |

| **Visie vooraf** | | |
|---|---|---|
| 10.2.E | 10.2.E | 10.2.E |
| Datum/paraaf | Datum/paraaf | Datum/paraaf |

**Gevraagde beslissing:**
Instemmen met:

1. Het conceptwetsvoorstel computercriminaliteit III, zoals aangepast naar aanleiding van de ingekomen adviezen;
2. Enkele beslispunten met betrekking tot het conceptwetsvoorstel;
3. Het Privacy Impact Assessment (PIA) bij het conceptwetsvoorstel;
4. Toezending van het conceptwetsvoorstel, met de PIA als bijlage, aan de CBVJ (behandeling op 2 januari 2014).

**Samenvatting:** Het conceptwetsvoorstel wordt positief ontvangen door politie en OM, de rechtspraak is welwillend maar de andere instanties zijn kritisch of afwijzend. De belangrijkste kritiekpunten betreffen nut en noodzaak van het binnentreden van computers, de toepassing van deze bevoegdheid buiten de landsgrenzen als niet bekend is waar de gegevens zich bevinden, nut en noodzaak van het decryptiebevel aan de verdachte en de positie van klokkenluiders bij heling van gegevens. Naar aanleiding van de adviezen is het wetsvoorstel op

enkele ondergeschikte punten aangepast. De belangrijkste wijzigingen betreffen de verruiming van de kring van opsporingsambtenaren die kunnen worden belast met het onderzoek in een geautomatiseerd werk, de verruiming van de uitzondering van strafbaarheid voor heling van gegevens voor klokkenluiders, de verruiming van de strafbaarstelling van grooming en de strafbaarstelling van online handelsfraude.

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

**Datum**
2 december 2013

**Ons kenmerk**
volgt

## Toelichting

1. Inleiding

Bij nota van 16 april is de inhoud van het conceptwetsvoorstel op hoofdlijnen geschetst. Deze nota is ter informatie bijgevoegd (kenmerk 377713).

Het conceptwetsvoorstel bevat de volgende onderdelen:
a) Het op afstand heimelijk binnentreden van computers, met het oog op (onder meer) het overnemen van gegevens, het ontoegankelijk maken van gegevens en het aftappen van communicatie;
b) Het decryptiebevel aan de verdachte bij ernstige vormen van kinderpornografie en terrorisme;
c) Aanpassing van de bestaande procedure voor het bevel aan de aanbieder van een communicatiedienst tot het ontoegankelijk maken van gegevens;
d) Strafbaarstelling van het wederrechtelijk overnemen (kopiëren) van gegevens en voorhanden hebben ("heling") van gegevens.

Op 2 mei 2013 is aan een aantal adviesorganen advies gevraagd over het wetsvoorstel computercriminaliteit III. Advies is ontvangen van het College van procureurs-generaal, de korpschef van de politie, de Raad voor de rechtspraak (Rvdr), de Nederlandse Vereniging voor Rechtspraak (NVvR), de Nederlandse Orde van Advocaten (NOvA) en Bits of Freedom (BoF). Daarnaast heeft de internetconsultatie ruim vijftig reacties opgeleverd, zowel van particulieren, bedrijven (Google, KPN), belangenbehartigers (Nederlands Juristen Comité voor de Mensenrechten, Nederlandse Vereniging van Journalisten, Nederland ICT) als overheidsinstanties (FIOD en Koninklijke marechaussee).

Het College bescherming persoonsgegevens (Cbp) heeft te kennen gegeven in dit stadium van het conceptwetsvoorstel geen advies uit te willen brengen. Het Cbp heeft verzocht om toezending van het naar aanleiding van de adviezen aangepaste conceptwetsvoorstel, zodat het Cbp daarover advies zou kunnen uitbrengen. Aan dit verzoek is geen gevolg gegeven; overeenkomstig uw standpunt in de discussie met het Cbp over de positie van dit orgaan in de consultatie van wetsvoorstellen.

In aanvulling op de bovengenoemde onderwerpen zijn de verruiming van de strafbaarstelling van de grooming en de strafbaarstelling van de online handelsfraude in het conceptwetsvoorstel opgenomen, conform uw toezeggingen ter zake aan de Kamer. Dit komt hieronder nader aan de orde.

2. De inhoud van de adviezen

Het College van procureurs-generaal en de politie zijn positief, de NVvR en de RvdR staan welwillend ten opzichte het conceptwetsvoorstel. De NOvA en BoF wijzen het wetsvoorstel af.

a) Het op afstand heimelijk binnentreden van computers (artikel II, onderdeel...)

Het College van procureurs-generaal onderstreept het belang van dit voorstel. De Raad voor de rechtspraak erkent de noodzaak van de voorgestelde bevoegdheid. De NOvA ziet hiervoor niet voldoende onderbouwing en Bof heeft een groot aantal bezwaren. Ook in de internetconsultatie worden nut en noodzaak van de voorgestelde bevoegdheid betwist. Daarbij wordt gewezen op de risico's die aan de toepassing van deze bevoegdheid zijn verbonden (aantasting privacy en controle op juiste werking van de software).
Naar aanleiding van de adviezen is in de memorie van toelichting ingegaan op de noodzaak van de voorgestelde bevoegdheid en de waarborgen voor een zorgvuldige inzet. Dit betreft paragraaf 2.3. (blz. )

In het oorspronkelijke voorstel kon het onderzoek in een geautomatiseerd werk uitsluitend worden verricht door een ambtenaar van politie. De politie beschikt daarvoor over IT-specialisten, die zijn ondergebracht in het team high tech crime (THTC). In de internetconsultatie hebben de Kmar en de FIOD aangedrongen op verruiming van de bevoegdheid, zodat ook de opsporingsambtenaren van de Kmar en de bijzondere opsporingsdiensten kunnen worden belast met het onderzoek in een geautomatiseerd werk. Idealiter zouden deze diensten gebruik moeten kunnen maken van de expertise van de politie, zoals bij het direct afluisteren, maar de Kmar en de BOD'en willen niet afhankelijk zijn van de prioriteitsstelling van de politie en dringen aan op de mogelijkheid van een zelfstandige inzet van deze bevoegdheid. Hieraan zijn politieke risico's verbonden, omdat u verantwoordelijk bent voor de rechtshandhaving en daarmee voor de kwaliteit van de opsporing door deze diensten. Aan de wensen van de Kmar en de bijzondere opsporingsdiensten kan tegemoet worden gekomen door bij of krachtens algemene maatregel van bestuur eisen te stellen aan de deskundigheid en positie (functiescheiding) van de opsporingsambtenaren die kunnen worden belast met het onderzoek in een geautomatiseerd werk. Het is dan verder aan de betrokken opsporingsdienst zelf om te bepalen of hiervoor capaciteit wordt vrijgemaakt.

**Beslispunt 1:**
Kunt u instemmen met de voorgestelde verruiming van de bevoegdheid tot de opsporingsambtenaar, die voldoet aan de bij of krachtens AMvB te stellen eisen op het gebied van deskundigheid.

In de toelichting is aangegeven dat, als de locatie van de gegevens niet bekend is, onder omstandigheden opsporingshandelingen kunnen worden verricht met betrekking tot die gegevens (bijvoorbeeld ontoegankelijk maken of overnemen). Verschillende adviesorganen (NOvA, NCJM, Bof) plaatsen kanttekeningen bij het verrichten van opsporingshandelingen rond gegevens waarvan de locatie niet bekend is. Hierbij wordt gewezen op de beginselen van het internationale recht en het risico van reciprociteit. Ook wordt gewezen op de kaders van het Cybercrimeverdrag. Het College acht dit vooral een academische discussie. Mede in het licht van de politieke discussie is, naar aanleiding van de adviezen, in de memorie van toelichting benadrukt dat de regering veel waarde hecht aan gemeenschappelijk optreden met andere staten en dat zelfstandig optreden van de opsporingsautoriteiten geen afbreuk mag doen aan bestaande afspraken op het gebied van de rechtshulp. Daarbij blijven de Nederlandse waarborgen

(machtiging RC en notificatieplicht) onverminderd gelden. Dit betreft paragraaf 2.8. (blz. ...)

b) Aanpassing van de procedure voor het ontoegankelijk maken van gegevens (artikel II, onderdeel ...)

Dit betreft aanpassing van de bestaande bevoegdheid van de officier van justitie om een aanbieder van een communicatiedienst te bevelen gegevens ontoegankelijk te maken voor zover noodzakelijk ter beeindiging van een strafbaar feit. Het OM adviseert de bevoegdheid te beperken tot ernstige strafbare feiten, waarvoor voorlopige hechtenis mogelijk is. Ook de NOvA vreest voor toepassing in bagatelzaken.
Aan deze adviezen is gevolg gegeven, vanwege de raakvlakken met de vrijheid van meningsuiting lijkt het verstandig de bevoegdheid te beperken tot ernstige strafbare feiten, waarvoor voorlopige hechtenis mogelijk is.

**Beslispunt 2:**
Kunt u instemmen met de beperking van de bevoegdheid van de officier van justitie, om gegevens ontoegankelijk te doen maken, tot ernstige strafbare feiten waarvoor voorlopige hechtenis mogelijk is.

c) Het decryptiebevel aan de verdachte (artikel I, onderdelen....)

Het College acht de beperking tot de twee delicten (kinderpornografie en terrorisme) wat willekeurig en adviseert uit te gaan van zeer ernstige strafbare feiten waarbij er aanwijzingen bestaan voor een concreet gevaar voor het leven of de vrijheid van een persoon of de veiligheid van de staat. Ook de NVvR denkt in deze richting.

De zienswijze van het College is op het eerste gezicht aantrekkelijk. Bezwaar is echter dat daarmee afstand wordt genomen van de brief aan de Kamer van 15 oktober 2012 en (vooral) van het TILT-rapport, dat in het licht van artikel 6 van het EVRM uitsluitend ruimte ziet voor een decryptiebevel aan de verdachte ingeval van verdenking van bepaalde ernstige strafbare feiten, die een maatschappelijk probleem vormen en waarbij de noodzaak van een dergelijk bevel is gebleken. Tot nu toe is er geen behoefte voor een decryptiebevel anders dan voor de bestrijding van kinderpornografie. Nu reeds kiezen voor verruiming van de reikwijdte van het decryptiebevel lijkt vanuit strategisch oogpunt dan ook weinig aantrekkelijk, omdat daarmee afstand wordt genomen van het TILT-rapport. Wel wordt in de memorie van toelichting sympathie betuigd voor het voorstel van het College. Daarbij wordt voorgesteld de toepassing voor terroristische misdrijven te beperken tot strafbare feiten waarop een gevangenisstraf van acht jaar of meer is gesteld, zodat het decryptiebevel in ieder geval is beperkt tot een zeer ernstig strafbaar feit.

**Beslispunt 3:**
Kunt u instemmen met (voorlopige) handhaving van de mogelijkheid van het decryptiebevel aan de verdachte tot de ernstige vormen van kinderpornografie en terrorisme, waarop een gevangenisstraf van acht jaar of meer is gesteld.

d) Strafbaarstelling van het wederrechtelijk overnemen van gegevens en van "heling" van gegevens (artikel I, onderdelen C en E)

OM en politie zijn positief over het voorstel voor de artikelen 139c en 139g Sr omdat dit voorziet in een al lang bestaande behoefte uit de praktijk. Dit biedt de mogelijkheid om personen strafrechtelijk aan te pakken die beschikken over grote aantallen creditcardgegevens zonder dat daarvoor een redelijke verklaring is.

Enkele adviesorganen (NOvA en Bof) hebben erop gewezen dat de uitzondering van strafbaarheid voor klokkenluiders verruiming behoeft, omdat deze is beperkt tot de bekendmaking van gegevens. Naar aanleiding van deze adviezen is de uitzondering van strafbaarheid verruimd tot alle strafbaar gestelde handelingen rond het helen van gegevens.

3. Aanvullende onderwerpen

a)De verruiming van de strafbaarstelling van grooming (artikel I, onderdeel...)

Tijdens de behandeling van de begroting van VenJ en in de beantwoording van Kamervragen is door u toegezegd dat de strafbaarstelling van grooming (art. 248e Sr: het benaderen van minderjarige op internet met het oogmerk seksuele handelingen net die minderjarige te verrichten) zal worden verruimd, zodat de inzet van een oudere lokpuber (een opsporingsambtenaar die zich op internet als minderjarige voordoet) mogelijk wordt. Ter uitvoering van die toezegging is een voorstel tot verruiming van de strafbaarheid van grooming in dit wetsvoorstel opgenomen: dit betreft het voorstel dat tevens degene strafbaar is die ten onrechte aanneemt met een minderjarige van doen te hebben. Die minderjarige kan dan in werkelijkheid een oudere persoon zijn, zoals de eerdergenoemde lokpuber. In de memorie van toelichting wordt aangegeven dat dit ook een virtuele persoon kan zijn. Eenzelfde verruiming wordt voorgesteld voor het delict van het corrumperen van een minderjarige (artikel 248d Sr), omdat het gebruik van een lokpuber daar ook aan de orde kan zijn.

De concepttekst is afgestemd met het OM en de nationaal rapporteur mensenhandel. Het OM kan zich in de tekst van de voorgestelde wijziging van artikel 248e Sr en de toelichting vinden.

b) De strafbaarstelling van de online handelsfraude (artikel I, onderdeel..)

In de beantwoording van Kamervragen is door u toegezegd te zullen onderzoeken in hoeverre online handelsfraude (het aanbieden van goederen op websites, zoals markplaats, zonder die te leveren) strafbaar dient te worden gesteld. Vervolging op grond van oplichting is doorgaans niet mogelijk vanwege de voor oplichting vereiste handelingen (valse naam of valse hoedanigheid, listige kunstgrepen of samenweefsel van verdichtsels). Naar aanleiding van nader overleg met het OM is een voorstel tot strafbaarstelling van de online handelsfraude in dit wetsvoorstel opgenomen: dit betreft het maken van een beroep of gewoonte van het aanbieden van goederen of diensten met het oogmerk na betaling niet te leveren. Door aan te sluiten bij het vereiste van het beroep of de gewoonte wordt voorkomen dat bagatelzaken voor vervolging in aanmerking kunnen komen (artikel 12-procedures). Bijkomend voordeel van strafbaarstelling is de mogelijkheid voor de slachtoffers zich met een vordering tot schadevergoeding in het strafproces te voegen.

Het OM kan zich in de tekst van het voorgestelde artikel 329d Sr en de toelichting vinden.

4. Het Privacy Impact Assessment

Mede ter uitvoering van de motie Franken is bij het wetsvoorstel een Privacy Impact Assessment (PIA) opgesteld. De PIA licht het wetsvoorstel door op risico's voor de bescherming van de persoonlijke levenssfeer en komt tot een aantal risicobeheersende maatregelen. Hoewel de meeste risico's door de genomen maatregelen stevig worden gereduceerd, blijven er 'restrisico's' over. De belangrijkste restrisico's van het wetsvoorstel zijn:

P.M.

De PIA wordt als bijlage bij het wetsvoorstel gevoegd en de daarin opgenomen risicobeheersende maatregelen worden door het wetsvoorstel afgedekt.

5. Afstemming

Het naar aanleiding van de adviezen aangepaste conceptwetsvoorstel is afgestemd met de NCTV en BZK/CZW. De aanvullende onderdelen (grooming en on line handelsfraude) zijn afgestemd met het OM.

De wetgevingstoets heeft plaatsgevonden; de opmerkingen zijn verwerkt.

++

# Nr. 004

Ministerie van Veiligheid en Justitie

De Minister van Veiligheid en Justitie

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

**Contactpersoon**[1]

*Raadadviseur*

T 10.2.E
10.2.E

**Datum**
3 februari 2014

**Ons kenmerk**
474762

**Dossiernummer**
377589

nota

Wetsvoorstel computercriminaliteit III aan Raad van State voor advies

**Algemene leiding**

| Minister | Staatssecretaris | SG |
|---|---|---|
| Datum/eindparaaf | Datum/paraaf | Datum/paraaf |

**Door tussenkomst van**

| DWJZ | Hoofd sector straf- en sanctierecht |
|---|---|
| Datum/paraaf | Datum/paraaf |

**Van**
10.2.E
Datum/paraaf

## Gevraagde beslissing:

Instemming met behandeling van het conceptwetsvoorstel computercriminaliteit III, met de Privacy Impact Assessment (PIA) bij het conceptwetsvoorstel als bijlage, in de RBJ van 11 februari 2014, met het oog op toezending aan de Raad van State voor advies.

## Toelichting

Dit conceptwetsvoorstel omvat enkele gevoelige voorstellen, zoals het op afstand heimelijk binnentreden van computers, met het oog op het verrichten van

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

**Datum**
3 februari 2014

**Ons kenmerk**
474762

bepaalde onderzoekshandelingen en de verruiming van de strafbaarstelling van grooming.

Het wetsvoorstel is in de CBVJ van 14 januari 2014 behandeld. De belangrijkste wijzigingen betreffen het volgende:

Op verzoek van het ministerie van BZK is in het conceptwetsvoorstel een evaluatiebepaling ingevoegd (Artikel III).

Op verzoek van het ministerie van Economische Zaken is de verhouding tussen de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk en het verbod op het plaatsen van cookies in artikel 11.7a van de Telecommunicatiewet expliciet geregeld. Dit heeft tevens geleid tot aanvulling van de memorie van toelichting op dit punt.

Op verzoek van het ministerie van Financiën is de financiële paragraaf aangevuld.

Inmiddels zijn met het College bescherming persoonsgegevens (Cbp) afspraken gemaakt over het advies van het Cbp. Dat advies is echter nog (steeds) niet binnen; het wordt volgende week verwacht. Bij deze stand van zaken is het raadzaam om het conceptwetsvoorstel alvast op de agenda van de RBJ te plaatsen. Als het advies van het Cbp daartoe aanleiding geeft, kan het conceptwetsvoorstel tussentijds worden aangepast.

++

# Nr. 005

Ministerie van Veiligheid en Justitie

Minister van Veiligheid en Justitie

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

**Contactpersoon**
10.2.E

10.2.E

nota

Verzending wetsvoorstel computercriminaliteit III aan de Raad van State

**Datum**
21 februari 2014

**Ons kenmerk**
484893

**Dossiernummer**
377589

**Algemene leiding**

| | |
|---|---|
| Minister | SG |
| Datum/eindparaaf | Datum/paraaf |

**Door tussenkomst van**

| | |
|---|---|
| DWJZ | Hoofd sector straf- en sanctierecht |
| Datum/paraaf | Datum/paraaf |

**Van**
10.2.E
Datum/paraaf

**Visie vooraf**

| | |
|---|---|
| 10.2.E | 10.2.E |
| Datum/paraaf | Datum/paraaf |

**Gevraagde beslissing:** instemming met (1) de verwerking van het advies van het College bescherming persoonsgegevens inzake het conceptwetsvoorstel computercriminaliteit III, en (2) verzending van het wetsvoorstel aan de Raad van State voor advies.

**Toelichting**

Het conceptwetsvoorstel computercriminaliteit bevat de volgende onderdelen:
a) Het op afstand heimelijk binnentreden van computers, met het oog op (onder meer) het verrichten van bepaalde opsporingshandelingen (onderzoek in een geautomatiseerd werk);

**Directie Wetgeving en Juridische Zaken**
sector straf- en sanctierecht

**Datum**
20 februari 2014

**Ons kenmerk**
484893

b) Het decryptiebevel aan de verdachte bij ernstige vormen van kinderpornografie en terrorisme;
c) Aanpassing van de bestaande procedure voor het bevel aan de aanbieder van een communicatiedienst tot het ontoegankelijk maken van gegevens;
d) Strafbaarstelling van het wederrechtelijk overnemen (kopiëren) van gegevens en voorhanden hebben ("heling") van gegevens.
e) Verruiming van de strafbaarstelling van 'grooming' (art. 248e Sr), zodat de inzet van een oudere lokpuber mogelijk wordt;
f) Strafbaarstelling van de on line handelsfraude (op websites aanbieden van goederen of diensten zonder te leveren).

Op 14 februari stemde de Ministerraad in het de verzending van het conceptwetsvoorstel computercriminaliteit III aan de Raad van State voor advies. Besloten is dat het conceptwetsvoorstel opnieuw in de Ministerraad worden besproken voordat het aan de Kamer wordt aangeboden.

Deze week is alsnog het advies van het College bescherming persoonsgegevens (Cbp) over dit conceptwetsvoorstel ontvangen. Het advies is bijgevoegd. Het advies is opgehouden vanwege de discussie met het Cbp over de positie van dit orgaan in de advisering over conceptwetsvoorstellen.

Het advies van het Cbp is – zoals te verwachten – kritisch. Het advies is echter beperkt tot het onderdeel van het onderzoek in een geautomatiseerd werk (punt a) en is op dat punt niet verstrekkend. Het Cbp acht nut en noodzaak van het onderzoek in een geautomatiseerd niet voldoende onderbouwd. Voorts verzoekt het Cbp om de beschikbaarstelling van statistische gegevens over de toepassing van deze bevoegdheid en opneming van een horizonbepaling.

Het advies van het Cbp is inmiddels verwerkt in het conceptwetsvoorstel. Naar aanleiding daarvan is de memorie van toelichting aangevuld. Dit betreft hoofdstuk 2 (Onderzoek in een geautomatiseerd werk) en hoofdstuk 9 (De adviezen). Nut en noodzaak zijn nader onderbouwd, daarbij wordt specifiek ingegaan op de problemen rond het vorderen van gegevens bij buitenlandse aanbieders. Het verzoek om beschikbaarstelling van statistische gegevens wordt gehonoreerd; naar het model van de tapgegevens kan jaarlijks een overzicht openbaar worden gemaakt. Opneming van een horizonbepaling is (vooralsnog) afgehouden; weliswaar voorziet het regeerakkoord in een horizonbepaling bij inbreuken door de overheid maar bij het wetsvoorstel ANPR is gebleken dat de fracties van de Tweede Kamer geneigd zijn een dergelijke bepaling op te vatten als een blijk van twijfel bij de indiener over de noodzaak van het eigen wetsvoorstel. Daarvan is bij dit conceptwetsvoorstel geen sprake.

Graag geef ik u in overweging in te stemmen met de verwerking van het advies van het Cbp en verzending van het conceptwetsvoorstel aan de Afdeling advisering van de Raad van State voor advies.

++

# Nr. 006

| | |
|---|---|
| **Van:** | 10.2.e - BD/DRC/CV |
| **Aan:** | 10.2.e - BD/DGPenV/PPM/BITE |
| **Cc:** | 10.2.e - BD/DRC/CV |
| **Onderwerp:** | FW: Stukje voor SG tbv google-diner |
| **Datum:** | woensdag 26 februari 2014 08:37:52 |

---

Hoi 10.2.e ,
Misschien toch iets te lang, maar hier is het stukje.
Groet,
10.2.e

De digitale wereld biedt niet alleen gewone burgers en organisaties veel mogelijkheden, maar ook criminelen. Het derde Cyber Security Beeld Nederland van juni 2013 benoemt cybercrime en cyber spionage als de twee grootste dreigingen. Om cybercrime en andere vormen van criminaliteit met gebruik van digitale middelen het hoofd te bieden is het Wetsvoorstel Computercriminaliteit III in voorbereiding. Bij het wetsvoorstel is een *privacy impact assessment* opgesteld om de gevolgen voor de privacy te duiden. Het wetsvoorstel is na de internetconsultatie recentelijk voor advies aan de Raad van State gestuurd. Voor de zomer wordt een reactie van de Raad van State verwacht.
Het wetsvoorstel behelst onder meer nieuwe bevoegdheden voor de politie, te weten om computers en systemen te hacken ("binnendringen in geautomatiseerd werk"), om elektronische gegevens ontoegankelijk te maken, en om een bevel tot decryptie van versleutelde gegevens aan een verdachte te geven. Deze bevoegdheden mogen volgens het wetsvoorstel alleen worden ingezet voor ernstige strafbare feiten. Het binnendringen in geautomatiseerd werk en het ontoegankelijk maken van gegevens is alleen toegestaan na machtiging van de rechter-commissaris. Deze bevoegdheden zijn nodig, omdat criminelen steeds vaker gebruik maken van de versleuteling van gegevens, anonimiseringstechnieken op internet zoals Tor, en de opslag van gegevens in de *cloud*.
Inhoudelijke discussiepunten zijn onder meer de inbreuk op de privacy bij het binnendringen in geautomatiseerd werk, de mogelijkheid binnen te dringen in systemen die fysiek niet op Nederlands grondgebied staan en het vastleggen van de handelingen bij het binnendringen. Deze discussiepunten worden in het wetsvoorstel geadresseerd.
Daarnaast regelt het voorstel de strafbaarstelling van het wedderrechtelijk overnemen en helen van gegevens, en het (herhaaldelijk) plegen van online handelsfraude.
Tenslotte verruimt het de strafbaarstelling voor *grooming*.
Buiten reikwijdte

# Nr. 008

**Grote zorgen Nederlandse internet- en technologiesector over hackwet**
*Position paper Wet Computercriminaliteit III*
Versie: 3 april 2015

De Nederlandse internet- en technologiesector[1] maakt zich ernstig zorgen over de aanstaande Wet Computercriminaliteit III waarin de overheid zichzelf de bevoegdheid geeft om te hacken. De sector begrijpt dat er soms nieuwe wetgeving nodig is waarmee de politie beter kan inspelen op nieuwe ontwikkelingen, maar is tegelijkertijd van mening dat nieuwe bevoegdheden altijd gekoppeld moeten worden aan scherpe waarborgen. De juiste balans tussen collectieve veiligheid en individuele vrijheden vereist dat inzet van dergelijke vergaande bevoegdheden scherp getoetst wordt. Over het gebruik ervan moet expliciet verantwoording afgelegd. Dat is in de conceptversie van de wet nog niet geborgd en is voor de sector wel een vereiste. Op deze manier veroorzaakt de wet een onevenredig grote inbreuk op grondrechten en enorme economische schade.

**Nieuwe bevoegdheid verstrekkend en weinig onderbouwd**
Met de nieuwe Wet Computertcriminaliteit III introduceert het kabinet een nieuwe bevoegdheid: het heimelijk binnendringen van een geautomatiseerd werk. Dit betekent concreet het mogen hacken van apparatuur zoals computers en mobiele telefoons, maar ook het hacken van clouds en slimme energiemeters valt onder de bevoegdheid. Ondanks de verstrekkendheid van dit alles wordt in de Memorie van Toelichting niet ingegaan op de noodzaak voor deze inbreuk. Een empirische onderbouwing voor het ‘waarom’ ontbreekt volledig. Ook de subsidiariteit en proportionaliteit worden niet toegelicht. De inzet is daarnaast niet beperkt tot terughacken en cybercrime, maar omvat alle misdaden vanaf een bepaalde strafmaat, inclusief delicten die raken aan de vrijheid van meningsuiting zoals bijvoorbeeld prikkelende cartoons en majesteitschennis. Daarbij wordt de inzet niet beperkt tot de Nederlandse landsgrenzen.

Scherpe waarborgen in de wet zijn juist in het digitale domein extra belangrijk. Traditionele remmen vanuit kosten en capaciteit gelden vrijwel niet wanneer een functionaliteit eenmaal bestaat en extra inzet praktisch gratis is. Het risico van grootschalige inzet is daarmee levensgroot. Dit vraagt om juridisch goed vormgegeven toezicht dat beschikt over voldoende middelen.

**Zowel inbreuk op grondrechten als economie**
Volgens de sector is dit voorstel in zijn huidige vorm een disproportionele inbreuk op de grondrechten van burgers, zoals het recht op privacy en de vrijheid van meningsuiting. Het brengt bovendien de vrije pers in gevaar omdat bronbescherming niet meer te garanderen is. Daarnaast voorzien we dat er flinke negatieve economische gevolgen kleven aan de nieuwe wet. Het vertrouwen in de Nederlandse internetinfrastructuur en -economie krijgt een flinke tik als deze wet doorgaat.

Nederland heeft nu een zeer sterke positie op het gebied van internet. Het vestigingsklimaat is goed en er ontstaan op het moment allerlei veelbelovende startups. We hebben deze sterke

---

[1] Nederland ICT, KPN, Vodafone, Ziggo, TomTom, Google, Microsoft, Nederlandse Uitgevers Verbond, Dutch Hosting Providers Association, Stichting Digitale Infrastructuur Nederland, Verizon Enterprise Solutions, SIDN, AMS-IX, Bureau Brandeis,

positie te danken aan het feit dat de bevolking hoog opgeleid is, praktisch iedereen voorzien is van snelle internetverbindingen (zowel vast als mobiel) en Nederland met AMS-IX beschikking heeft over een van de grootste internetknooppunten ter wereld. Recente investeringen van grote bedrijven als Google, IBM en Microsoft en het flinke aantal techstartups onderschrijven de sterke positie van Nederland en het vertrouwen dat bestaat in de Nederlandse internet en technologiesector.

**Ondermijning vertrouwen en vestigingsklimaat**
De bevoegdheid van de overheid om apparatuur te hacken schaadt de goede positie van Nederland enorm. De voorstellen beperken zich niet tot eindgebruikers, maar geven ook bevoegdheden om binnen te dringen in gedeelde clouds, “Internet of Things” en autonoom rijdende auto’s met een data verbinding. Bedrijven die actief zijn in Nederland en hier bijvoorbeeld datacentra hebben of netwerkdiensten aanbieden kunnen dan niet langer de integriteit van hun systemen, diensten en data garanderen. Het gevolg is verlies van het vertrouwen van klanten en mogelijk een vertrek uit Nederland. Ook zal het aantal succesvolle startups afnemen. Dit effect wordt enkel sterker als andere landen in de Nederlandse ambitie ook over de grens te hacken de legitimatie vinden om in te breken op Nederlandse computers.

**Graag meedenken over betere waarborgen**
De Nederlandse internet- en technologiesector denkt graag mee hoe het wetsvoorstel beter vormgegeven kan worden door middel van betere waarborgen. Daarom presenteren wij hieronder enkele voorstellen. Verschillende van de betrokken partijen hebben daarnaast nog zorgen over andere gedeeltes van deze wet. Zij hebben dat in de consultatiefase al aangegeven en zullen dat de komende periode kenbaar blijven maken.

**Waarborgen, toetsing en verantwoording verbeteren door:**
- Betere afbakening van het begrip geautomatiseerd werk;
- Inzet enkel bij een kleinere set beter afgebakende zware misdrijven;
- Enkel speciaal opgeleide opsporingsambtenaren inzetten;
- Inzet beperken tot apparaten gelokaliseerd in Nederland (plus parallel verbeteren en versnellen van rechtshulpverdragen);
- De eis dat het geautomatiseerd werk daadwerkelijk is gebruikt voor een strafbaar feit;
- De bevoegdheid mag enkel worden uitgeoefend met een geschikt technisch hulpmiddel;
- Vooraf vindt een impact analyse plaats;
- Aangetroffen gegevens van derden mogen enkel bewaard indien ze in relatie staan tot het strafbare feit;
- Een nieuwe expertgroep voor de rechter commissarissen die gaan over de inzet van de bevoegdheid;
- Een verplichting voor rechter-commissarissen om deskundigen te benoemen;
- Een instructie voor de rechter commissaris dat vrijheid van meningsuiting en bronbescherming zwaarwegende belangen zijn;
- De machtiging om de bevoegdheid uit te oefenen is altijd ‘met redenen omkleed’;
- Een kortere standaard termijn voor uitoefening van de bevoegdheden;
- Verlenging enkel mogelijk indien het verzoek schriftelijk is en ‘met redenen omkleed’;
- De plicht om uitoefening van bevoegdheden te beëindigen als niet meer aan de voorwaarden wordt voldaan;

- Een verbod onderzoek te doen naar gegevens van verschoningsgerechtigden, journalisten en hun bronnen;
- Te allen tijde dient te kunnen worden gecontroleerd welke technische handelingen in het kader van de opsporing in het desbetreffende geautomatiseerde werk hebben plaatsgevonden;
- Betrokken netwerkpartijen dienen genotificeerd te worden;
- Belanghebbenden kunnen zich beklagen;
- Voldoende middelen om het toezicht op de bevoegdheid effectief en efficiënt in te vullen;
- Een horizonbepaling in de wet;
- Het ‘Besluit technische hulpmiddelen strafvordering’ waarin de invulling van de bevoegdheid wordt uitgewerkt moet tegelijkertijd behandelt in de Tweede Kamer en voorzien van een zware voorhangprocedure.

**Ondertekenaars:**
Nederland ICT, KPN, Vodafone, Ziggo, TomTom, Google, Microsoft, Nederlandse Uitgevers Verbond, Dutch Hosting Providers Association, Stichting Digitale Infrastructuur Nederland, Verizon Enterprise Solutions, SIDN, AMS-IX en Bureau Brandeis.

Nr. 009

Dossier gesprek Stas – Google 27 mei 2015

**Wetsvoorstel computercriminaliteit III**

Spreekpunten

- Om de opsporing en vervolging van computercriminaliteit te versterken zijn maatregelen nodig, die beter aansluiten bij de snelle ontwikkeling op het terrein van technologie, internet en computercriminaliteit. Bestaande wetgeving is verouderd en biedt onvoldoende mogelijkheden om bijvoorbeeld versleuteling van gegevens ongedaan te maken, illegale acties op het internet aan te pakken of kinderpornografie online te bestrijden.
- Versterking van opsporing en vervolging is nodig:
    - In gelijke tred van de algehele digitalisering van de samenleving neemt computercriminaliteit toe en zijn politie en OM steeds meer afhankelijk van electronisch bewijs.
    - Dat het vanwege de vaak grensoverschrijdende (internationale) crime scenes, en door het zich anoniem op internet kunnen bewegen, en of, door niet voor derden leesbare communicatie te wisselen, mag niet leiden to straffeloosheid op internet en het ontstaan van zogenoemde safehavens voor internetcriminaliteit. De samenleving, burgers en bedrijven en hun belangenmoeten worden beschermd.
- Op afstand en heimelijk betreden van computers is in dit verband een nieuw te introduceren bevoegdheid die de opsporing en vervolging en het effect daarvan belangrijk zal versterken.
- Maar natuurlijk wel binnen het raamwerk van de rechtstaat. De regering, het parlement en de Nederlandse burger hechten veel belang aan privacy.
- In het wetsvoorstel computercriminaliteit III, zijn daarom - mede als gevolg van opmerkingen van Google en andere belanghebbenden – veel waarborgen opgenomen, zoals een drempel voor de inzet (alleen ernstige misdrijven), goedkeuring door de Officier van Justitie en specifieke machtiging door de Rechter Commissaris. Ook zal de uitvoering van de bevoegdheid streng zijn geprotocolleerd om misbruik van de bevoegdheid te voorkomen.
- Het wetsvoorstel wil ik voor het zomerreces (juli) aan het parlement sturen.

Achtergrond

Google en andere ICT diensten providers hebben zich tot nu toe veelal tegenstander van CC III getoond. Ze vrezen een verlies van (vertrouwen van) klanten en daarmee een teruglopende markt. Maar ook vrezen zij aantasting van de betrouwbaarheid en, of capaciteiten van hun eigen netwerken, in het geval die betreden worden.

Tijdens de consultatiefase, maar ook soms in bijdragen op congressen of in andere fora, geeft Google deze boodschap af.

Al vanaf de consultatie van het ontwerp wetsvoorstel en zeker ook na het advies van de Raad van State, is nog goed gekeken hoe deze en vergelijkbare vrees kan worden weggenomen. In de vorm van strenge waarborgen en goede protocollering van de uitvoering menen DGRR en DWJZ dat dat kan.
Ik wijs op:

1. Het gaat om ernstige strafbare feiten (art. 67 Sv)
2. De OvJ geeft een bevel op voordacht van een concreet project door de politie
3. De RC moet een machtiging geven voor dat het bevel kan worden uitgevoerd
4. Er zijn tijdsbeperkingen aan de uitvoering en voor elke nieuwe handeling (bijvoorbeeld opvernmen in aanvulling op het bekijken (“opnemen”) van de plaats is een nieuw bevel en machtiging nodig.
5. Er zal sprake zijn van een geprotocolleerde inzet, met zoveel mogelijk gecertificeerde middelen.

Dossier gesprek Stas – Google 27 mei 2015

# Nr. 010

**Verslag bilateraal gesprek Staatssecretaris met Google**

Datum: 27 mei 2015
Aanwezig:
Google: 10.2.e , 10.2.e , 10.2.e
VenJ: Staatssecretaris Dijkhoff, 10.2.e (DCS), 10.2.e (DCS)

*Voorstellen en kennismaken*
Staatssecretaris Dijkhoff geeft de intentie aan een goede relatie met Google te willen hebben, die meer is dan ontmoeten en weer weggaan. Hij onderstreept de belangen van een open, vrij en veilig internet waarin ruimte is voor ontwikkeling van het bedrijfsleven. 10.2.e geeft aan dat deze belangen gedeeld worden. Als hij in Europa is ervaart hij een somber gevoel over dat laatste, waarin hij hoort dat mensen vinden dat de oorlog over internet is verloren. Google vindt dit niet terecht en wijst op de mogelijkheden en waarde van start-ups en grow-ups die ook in Europa bestaan. Google zoekt naar mogelijkheden om op dit gebied bij te dragen aan publiek-private initiatieven.

*Wetsvoorstel computercriminaliteit III*
10.2.e geeft aan dat de ideeën over toegang tot systemen verlenen aan de politie op afstand in WCC III een slecht idee is en zoekt communicatie hierover. Staatssecretaris Dijkhoff geeft aan de bezwaren te kennen, maar dat hij een bredere afweging maakt. De ontwikkelingen gaan snel, en vergen veel inspanning om de infrastructuur veilig te houden, maar ook het gebruik van de infrastructuur (Staatssecretaris Dijkhoff gebruikte hier de tweedeling die de WRR in hun rapport aangeven: techniek versus gebruik).
Datzelfde geldt voor het gebruik van encryptie en bijdragen aan het afgeven van sleutels.

Google ondersteunt de insteek dat er geen crypto verbod of ontsleutelingsgebod komt om op deze manier cyberspace juist te kunnen beveiligen.

*Internationale samenwerking*
Buiten reikwijdte

*Samenwerking*

Buiten reikwijdte

*EU Data Protection*

Buiten reikwijdte

Buiten reikwijdte

# Nr. 011

**Van:** 10.2.e - BD/NCTV/DCS/ACSB
**Aan:** 10.2.e - BD/DCS; 10.2.e - BD/DGSB/AI; 10.2.e - BD/DCS/NCSC/AMR; 10.2.e - BD/NCSC; 10.2.e - BD/DCS/NCSC/AEA; 10.2.e - BD/DCS/NCSC/AMP; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRB/SBA; 10.2.e - BD/DGPenV/PPM/BITE; 10.2.e - BD/PSD; 10.2.e - BD/NCTV/DCS/ACSB; 10.2.e - BD/DNV; 10.2.e - BD/DNV
**Onderwerp:** terugkoppeling gesprek stas 10.2.e
**Datum:** dinsdag 9 juni 2015 12:08:52

---

Beste allen,

Hierbij de terugkoppeling van het gesprek vanochtend tussen Dijkhof en 10.2.e van Fox-IT. De politiek assistent was ook aanwezig. Vooral CC3 is een aandachtspunt voor de opvolging.

1) Accreditatie van bedrijven: Buiten reikwijdte
2) Responsible disclosure: Buiten reikwijdte
3) VS safety act/boetes: Buiten reikwijdte
4) CC3: 10.2.e was benieuwd hoe het daarmee stond en of het wetsvoorstel nog wordt aangepast. 10.2.e gaf aan dat hij van mening is dat de hackbevoegdheden smaller zouden moeten worden ingezet voor alleen cybercrime ipv breder voor ook andere vormen van criminaliteit. Hij schatte in dat decryptiebevel de eindstreep in de Kamer niet zou halen. Er is ook van gedachte gewisseld over jurisdictie. De staatsecretaris gaf aan dat hij binnenkort een briefing heeft over CC3 en dat gekeken moet worden naar vorm en timing. Ook met betrekking tot jurisdictie gaf de staatsecretaris het spanningsveld weer tussen juridische vorm en werkbaarheid ervan. Belangrijk om voor de briefing deze week in gedachte te houden is dat de staatsecretaris de facto aangaf dat het wetsvoorstel nog aangepast gaat worden.
5) Spionage: Buiten reikwijdte

Buiten reikwijdte

Groeten,

10.2.e

10.2.e
Directie Cyber Security
10.2.e @nctv.minvenj.nl
10.2.e

# Nr. 012

vodafone

Ministerie van Veiligheid en Justitie
T.a.v. de heer mr. G.A. van der Steur
Postbus 20301
2500 EH DEN HAAG

Vodafone
Simon Carmiggeltstraat 6
1011 DJ AMSTERDAM
www.vodafone.nl

datum 15 juni 2015
plaats Amsterdam
referentie JK150615

Excellentie, Geachte heer Van der Steur,

Allereerst wil ik u namens Vodafone Nederland van harte feliciteren met uw benoeming tot minister van Veiligheid en Justitie. Wij wensen u alle succes met de uitdagende onderwerpen die onder uw verantwoordelijkheid vallen. Onderwerpen die ook de nadrukkelijke belangstelling van Vodafone Nederland hebben. Graag leveren wij vanuit onze expertise en betrokkenheid een bijdrage aan relevante beleidsontwikkelingen. Om deze reden zouden wij u graag willen verzoeken tot een gesprek om kennis te maken. In dit gesprek willen we graag met u van gedachten wisselen over de volgende actuele ontwikkelingen.

**Transparantie over het aantal vorderingen van Nederlandse opsporingsdiensten**

Buiten reikwijdte

**Wet bewaarplicht telecomgegevens**
Buiten reikwijdte

**Wet Computercriminaliteit III**
Tenslotte heeft ook de Wet Computercriminaliteit III waarin de overheid zichzelf de bevoegdheid geeft om te hacken, onze belangstelling. Wij begrijpen dat er soms nieuwe wetgeving nodig is waarmee de politie beter kan inspelen op nieuwe ontwikkelingen om zo de veiligheid van burgers te garanderen. Tegelijkertijd zijn wij van mening dat nieuwe bevoegdheden altijd gekoppeld moeten worden aan scherpe waarborgen. Ook dient eventuele ongewenste technische en administratieve impact zoveel mogelijk beperkt te zijn. Inzet van dergelijke vergaande bevoegdheden dient scherp getoetst te worden en over het gebruik ervan moet expliciet en controleerbaar verantwoording afgelegd. Dat is in de conceptversie van de wet naar onze mening onvoldoende geborgd. Op deze manier veroorzaakt de wet een onevenredig grote inbreuk op grondrechten en kan grote economische schade ontstaan als vertrouwen van burgers en bedrijven of de stabiliteit van systemen worden geschaad . Wij denken graag constructief mee hoe het wetsvoorstel beter vormgegeven kan worden door middel van betere waarborgen.

Ik zou het zeer op prijs stellen wanneer u deze persoonlijke uitnodiging in overweging wilt nemen. Graag neemt mijn collega 10.2.e hiertoe contact op met uw secretariaat.

Met vriendelijke groet

10.2.e

10.2.e Vodafone Nederland

Cc: mr. dr. K.H.D.M. Dijkhoff (Staatssecretaris)

# Nr. 013

Ministerie van Veiligheid en Justitie

Staatssecretaris van VenJ

Cc Minister van VenJ

Sector straf- en sanctierecht
**Contactpersoon**
10.2.E

**Datum**
30 juni 2015

**Ons kenmerk**
volgt

**Dossiernummer**
volgt

nota

Wetsvoorstel computercriminaliteit III

**Algemene leiding**
Staatssecretaris | SG
Datum/eindparaaf | Datum/paraaf

**Door tussenkomst van**
DWJZ | Hoofd sector- straf- en sanctierecht
Datum/paraaf | Datum/paraaf

**Van**
10.2.E

Datum/paraaf

**Kopie aan**
Minister van VenJ
Datum/paraaf

**Gevraagde beslissing:** instemming met:
a. het concept voor het nader rapport inzake het conceptwetsvoorstel computercriminaliteit III;
b. enkele beslispunten met betrekking tot het nader rapport.

## 1. Inleiding

Het conceptwetsvoorstel computercriminaliteit III bevat de volgende onderdelen:
a) Het op afstand heimelijk binnentreden van computers, met het oog op (onder meer) het overnemen van gegevens, het ontoegankelijk maken

van gegevens en het aftappen van communicatie (Artikel II, onderdelen J, Q en W);
b) Het decryptiebevel aan de verdachte bij ernstige vormen van kinderpornografie en terrorisme (Artikel I, onderdeel F, en Artikel II, onderdeel C);
c) Aanpassing van de bestaande procedure voor het bevel aan de aanbieder van een communicatiedienst tot het ontoegankelijk maken van gegevens (Artikel I, onderdeel A, en Artikel II, onderdeel E);
d) Strafbaarstelling van het wederrechtelijk overnemen (kopiëren) van gegevens en voorhanden hebben ("heling") van gegevens (Artikel I, onderdelen C en E);
e) Verruiming van de strafbaarstelling van verleiding van een minderjarige tot ontucht en van grooming in verband met de inzet van de lokpuber (Artikel I, onderdelen G en H );
f) Strafbaarstelling van de online handelsfraude (Artikel I, onderdeel J).

De Raad van State is kritisch over de waarborgen rond het onderzoek in een geautomatiseerd werk en wijst het decryptiebevel aan de verdachte af. Dit leidt tot een dictum 4 (niet zenden, dan nadat). Aan de meeste opmerkingen van de Raad van State kan goed tegemoet worden gekomen. Een gevoelig punt is of de bevoegdheid van het binnendringen in een geautomatiseerd werk kan worden beperkt tot zeer zware misdrijven, waarvoor een gevangenisstraf van acht jaar of meer kan worden opgelegd, of dat het huidige voorstel gehandhaafd wordt (alle misdrijven waarvoor voorlopige hechtenis mogelijk is). Ook het aanvullend toezicht op de toepassing van deze bevoegdheid vormt een punt van aandacht, vanwege de gesprekken met de procureur-generaal bij de Hoge Raad in het kader van de dataretentie. 10.2.G

Vanwege het dictum van de Raad van State en de eerdere besluitvorming in de Ministerraad moet het conceptwetsvoorstel opnieuw worden voorgelegd aan de Ministerraad.

## 2. De belangrijkste punten van het advies

De belangrijkste punten van het advies betreffen het volgende:

2.1. Differentiatie van de voorwaarden voor onderzoek in een geautomatiseerd werk

In het wetsvoorstel wordt voorgesteld dat een opsporingsambtenaar, ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, op bevel van de officier van justitie en na machtiging van de rechter-commissaris op afstand heimelijk kan binnendringen in een geautomatiseerd werk, met oog op het verrichten van bepaalde onderzoekshandelingen. Dit betreft het identificeren van het informatiesysteem, het overnemen van gegevens, het aftappen van communicatie, het direct afluisteren en het gebruik van een mobiele telefoon als peilzender zodat de locatie daarvan (en die van de bezitter)

kan worden bepaald. Vereist is een machtiging van de rechter-commissaris.

De Raad van State staat niet afwijzend ten opzichte van de voorgestelde bevoegdheid ("onderschrijft dat bij de bestrijding van ernstige misdrijven binnen de grenzen van het grondwettelijk en verdragsrechtelijk beschermde recht op eerbiediging van de persoonlijke levenssfeer ook van de nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt") maar heeft kritiek op het feit dat de voorwaarden voor de toepassing van de verschillende onderzoekshandelingen uniform zijn, terwijl de inbreuk op de persoonlijke levenssfeer verschillend is. De Raad acht die voorwaarden voor de meeste onderzoekshandelingen voldoende. Dit geldt echter niet voor het doorzoeken van het geautomatiseerde werk en/of het kopiëren van gegevens; de inbreuk op de persoonlijke levenssfeer is volgens de Raad dan vergelijkbaar met het binnendringen van een woning om gesprekken af te luisteren. Daarvoor is vereist de verdenking van een strafbaar feit waarvoor acht jaar gevangenisstraf of meer is gesteld. De Raad acht eenzelfde drempel wenselijk voor het doorzoeken en overnemen van gegevens. Hiermee wordt dan tevens tegemoet gekomen aan de vereisten van proportionaliteit die uit het EVRM voortvloeien (art. 8 EVRM).

*Voorgestelde reactie*
Het advies van de Raad van State kan bezwaarlijk worden overgenomen omdat het kopiëren van gegevens ook nodig is in gevallen waarin sprake is van een voorlopige hechtenismisdrijf, zoals het beëindigen van een botnet. Een waarborg wordt gevonden in de afweging van de noodzaak en proportionaliteit van de inzet van de bevoegdheid door de officier van justitie en de rechter-commissaris. De beoogde onderzoekshandelingen worden in het bevel opgenomen en maken derhalve deel uit van die afweging. Daarbij wordt erop gewezen dat voor de huiszoeking in een woning in beginsel een machtiging van een rechter-commissaris is vereist. Daarbij kan de gehele computer, met alle opgeslagen gegevens, in beslag worden genomen.

**Beslispunt 1**
Kunt u ermee instemmen dat geen gevolg wordt gegeven aan het advies en dat wordt vastgehouden aan het algemene vereiste van een strafbaar feit waarvoor voorlopige hechtenis mogelijk is, zonder dat wordt gedifferentieerd naar de verschillende onderzoekshandelingen.

2.2. Het toezicht op de uitoefening van de bevoegdheid

De Raad van State wijst erop dat de ontwikkeling van de informatie- en communicatietechnologie mogelijkheden biedt tot het grootschalig vergaren en opslaan van persoonsgegevens ten behoeve van opsporing en vervolging, zoals de dataretentie en de ANPR en acht structureel toezicht wenselijk op de uitoefening van opsporingsbevoegdheden in zaken waarbij van informatie- en communicatietechnologie gebruik is gemaakt en die niet aan de rechter worden voorgelegd. Dit aanvullend toezicht dient zich te richten op het systeem waarbij een jaarlijkse openbare rapportage is aangewezen, naar het model van de CTIVD voor

de inlichtingen- en veiligheidsdiensten. Een dergelijk orgaan kan worden ondergebracht bij het OM, naar het voorbeeld van de Centrale Toetsingscommissie voor bijzondere opsporingsbevoegdheden (CTC), met een externe onafhankelijke voorzitter.

*Voorgestelde reactie*
Het aanvullend systeemtoezicht wordt afgehouden, volstaan wordt met een verwijzing naar de waarborgen rond de inzet van de bevoegdheid (rechterlijke toestemming vereist) en de jaarlijkse rapportage aan de Kamer omtrent die inzet (naar het model van de rapportages over het aftappen). In de discussie over het aanvullend toezicht op de toepassing van de bevoegdheden rond de dataretentie dient het advies voor het wetsvoorstel CC III echter als uitgangspunt. Bij de dataretentie is het voornemen om aanvullend toezicht te beleggen bij de procureur-generaal bij de Hoge Raad. Deze oriëntatie is van groot belang voor die over de toepassing van de bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk. Immers, het ligt voor de hand dat de Kamer zal aandringen op een soortgelijk toezicht op de toepassing van die bevoegdheid.

**Beslispunt 2**
Kunt u ermee instemmen dat aan het advies van de Raad van State over de ontwikkeling van aanvullend toezicht op de toepassing van de bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk niet wordt gevolgd en dat (voorlopig) wordt volstaan met verwijzing naar de bestaande waarborgen?

2.3. Het decryptiebevel aan de verdachte

Voorgesteld wordt dat de officier van justitie ingeval van verdenking van enkele zeer ernstige strafbare feiten, te weten het maken van een beroep of gewoonte van het bezit, de vervaardiging en de verspreiding van kinderpornografie en een terroristisch misdrijf, aan de verdachte een bevel kan geven tot ontsleuteling van versleutelde gegevens. Vereist is een machtiging van de rechter-commissaris. Op het niet meewerken wordt een gevangenisstraf gesteld van drie jaar.

De Raad van State acht de noodzaak van een decryptiebevel aan de verdachte niet duidelijk. Dit klemt temeer daar het onderzoek in een geautomatiseerd werk een dergelijk decryptiebevel overbodig maakt. Ook twijfelt de Raad van State aan de effectiviteit van een bevel aan de verdachte, vanwege mogelijke bewijsproblemen (bewijs van het opzet). Voorts wordt onvoldoende gemotiveerd dat het decryptiebevel 'EVRM-proof' is; omdat niet wordt ingegaan op eerdere uitspraken va het EHRM waarin een strafbedreiging van zes maanden een zodanig mate van dwang oplevert dat het nemo tenetur beginsel is aangetast (zaak Mc Guiness en Quinn tegen Ierland). De Raad van State adviseert een en ander beter te motiveren en anders het decryptiebevel aan de verdachte te schrappen.

*Voorgestelde reactie*
De Raad van State merkt terecht op dat nut en noodzaak niet voldoende zijn onderbouwd; het decryptiebevel aan de verdachte komt vooral tegemoet aan een politieke wens. De opsporingspraktijk geeft de voorkeur aan het onderzoek in een geautomatiseerd werk, mede vanwege mogelijke bewijsproblemen. In het licht van de jurisprudentie van het EHRM lijkt de voorgestelde strafmaat inderdaad nauwelijks houdbaar; het EHRM achtte destijds een strafbedreiging van zes maanden voor het niet voldoen door een verdachte van een aanslag aan een vordering tot het verstrekken van informatie over zijn bewegingen gedurende een bepaalde periode rond die aanslag in strijd met het beginsel van nemo tenetur. Niettemin lijkt het vanuit politiek opzicht nuttig het decryptiebevel aan de verdachte voorlopig te handhaven; de Kamer kan daarover dan zelf oordelen. Daar komt bij dat in het Verenigd Koninkrijk goede ervaringen zijn opgedaan met deze maatregel. Vanwege de vereisten van het EVRM wordt voorgesteld het decryptiebevel aan de verdachte verder te beperken, namelijk tot gevallen waarin er aanwijzingen zijn van risico's voor de gezondheid van personen of de veiligheid van de staat. Het nut van dit bevel voor de opsporingspraktijk wordt daarmee wel verder verminderd.

**Beslispunt 3**
Kunt u instemmen met handhaven van het decryptiebevel aan de verdachte, met dien verstande dat het decryptiebevel aan de verdachte vanwege de jurisprudentie van het EVRM verder wordt beperkt?

## 3. Overige aandachtspunten

3.1. Onderzoek in een geautomatiseerd werk en rechtsmacht

In de memorie van toelichting bij het wetsvoorstel wordt ingegaan op de verhouding tussen opsporingshandelingen in cyberspace en rechtsmacht (par. 2.8.). Het is betrekkelijk eenvoudig om vanuit een ander land via het internet strafbare feiten te plegen, waarbij de gevolgen zich in Nederland voordoen (trojans, botnets, DDOS-aanvallen), dan wel op moeilijk concreet te lokaliseren servers buiten Nederland data op te slaan die betrekking hebben op strafbare feiten waarvoor Nederland rechtsmacht heeft. De politie heeft behoefte aan de mogelijkheid om tegen deze strafbare feiten te kunnen optreden, bijvoorbeeld door gegevens te onderzoeken die zijn opgeslagen op een server. Vanwege de ontwikkeling van de Cloud en versleutelingstechnieken en anonimiseringstechnieken (TOR) is het niet altijd vast te stellen waar gegevens zich bevinden. In de toelichting wordt aangegeven dat in die gevallen heimelijk en op afstand in een geautomatiseerd werk kan worden binnengetreden, als het onderzoeksbelang daartoe aanleiding geeft en een zekere inspanning is verricht om de locatie van de gegevens vast te stellen. Zodra wetenschap bestaat dat de gegevens zich in een andere rechtsmacht bevinden dan wordt een verzoek om rechtshulp

gedaan zodra dat redelijkerwijs mogelijk is, waarbij aan de bevoegde buitenlandse autoriteiten verantwoording wordt afgelegd over de handelingen die worden verricht en de afwegingen die daarbij worden gemaakt.

De Raad van State heeft in het advies begrip voor de noodzaak om op te kunnen treden in gevallen waarin de feitelijke locatie van gegevens niet valt te achterhalen maar dringt aan op wettelijke regeling van procedurele aspecten en nadere uitleg in de toelichting. Hieraan is deels gevolg gegeven. In de memorie van toelichting is vermeld dat bij grensoverschrijdende handelingen rechtshulp het uitgangspunt blijft. Indien de gegevens zich in het buitenland bevinden, of wanneer de locatie onbekend is, dan dient dit te worden vermeld in het bevel, zodat het deel uitmaakt van de afweging van de officier en de rechter-commissaris over de inzet van de bevoegdheid.

**Onderzoek WODC naar rechtsmacht en cybercrime**
In een in opdracht van het WODC verricht onderzoek naar de rechtmatigheid binnen internationaal recht van grensoverschrijdende toegang tot data[1] is kritiek uitgeoefend op het wetsvoorstel. Volgens de onderzoekers gaat het wetsvoorstel verder dan het absoluut noodzakelijke voor grensoverschrijdend onderzoek. Dit rapport is (vooralsnog) niet aan de Kamer aangeboden, maar wel openbaar gemaakt door middel van publicatie op de website van het WODC.

In het rapport wordt beargumenteerd dat in de strikte - en dominante – klassieke interpretatie van het internationale recht iedere unilaterale bewijs verkrijgende activiteit in een buitenlandse staat als inbreuk op de soevereiniteit wordt beschouwd. Hier is volgens de onderzoekers sprake van een impasse.

De onderzoekers bevelen aan om het vraagstuk van de soevereiniteit in cyberspace op internationaal niveau te erkennen. Zij stellen voor dat een of twee staten, of een groep van staten het voortouw nemen in het ontwikkelen van een alternatieve uitleg van de huidige juridische kaders, die aansluit bij een niet doctrinaire benadering van internationaal recht, waarbij de rechtmatigheid van de statelijke handelingen wordt beoordeeld naar de kracht van de daarbij gehanteerde juridische argumenten.

De onderzoekers zijn van mening dat het wetsvoorstel CC III een stap in deze richting zet, maar geen aannemelijke argumenten voor een andere benadering aandraagt, omdat het aanzienlijk verder gaat dan strikt noodzakelijk is voor grensoverschrijdend cyberonderzoek. Volgens de onderzoekers kan het wetsvoorstel verbeterd worden door de reikwijdte te versmallen (bv. wel overnemen data, niet verwijderen data), meer waarborgen te verschaffen (bv. waar mogelijk notificeren van staten) en

[1] Cyberspace, de cloud en grensoverschrijdende opsporing: de grenzen en mogelijkheden van internationaal recht, 2015, Universiteit van Utrecht, Bert-Jan Koops, Morag Goodwin. Dit onderzoek is een vervolg op een eerder onderzoeksrapport over opsporing in de Cloud (Misdaad en opsporing in de wolken, 2012).

een betere onderbouwing te geven van wat als minimale inspanning mag worden gezien om de locatie van de data te achterhalen.

Het is niet uitgesloten dat de Kamer het vraagstuk van de rechtsmacht alsmede de verbetervoorstellen uit het onderzoek aan de orde zal stellen bij de parlementaire behandeling van het wetsvoorstel CC III. De suggesties van de onderzoekers zijn beperkend voor de inzet van de bevoegdheid in de praktijk, gelet hierop wordt hiermee vooralsnog terughoudend omgegaan. Indien nodig kunnen bij de parlementaire behandeling aanpassingen overwogen worden.

De onderzoekers bevelen aan om op de langere termijn te streven naar het creëren van een internationaal bindend instrument. Het onderzoeksrapport wordt gebruikt om in internationaal overleg de discussie op dit punt aan te jagen. Dit gebeurde eerder dit jaar tijdens de GCCS 2015 en zal opnieuw gebeuren op een hoog ambtelijke expertbijeenkomst tijdens het Nederlands EU-voorzitterschap in 2016.

3.2. Grooming

Voorgesteld werd de delictsomschrijving van grooming, het via internet benaderen door volwassenen van kinderen voor seksuele doeleinden, aan te passen om de inzet van een lokpuber (een opsporingsambtenaar die zich voordoet als minderjarige) mogelijk te maken. Ook strafbaar is degene die ten onrechte aanneemt met een minderjarige van doen te hebben. De formulering van de wetswijziging is op kritiek gestuit van het openbaar ministerie (OM), omdat het de inzet van de lokpuber nog steeds niet mogelijk zou maken . Kern van het bezwaar is dat bewijsproblemen zouden ontstaan omdat het oogmerk van de verdachte was gekoppeld aan de ontucht met de persoon met wie de afspraak wordt gemaakt (‘identiciteit’). Bij een oudere lokpuber knelt dit, omdat het oogmerk niet gericht is op het plegen van ontucht met de volwassen lokpuber, maar met een minderjarige.

Naar aanleiding van de kritiek is, in overleg met het OM, de tekst van de delictsomschrijving aangepast. Daarbij is het vereiste van de identiciteit losgelaten, zodat de afspraak met de lokpuber bewijsrechtelijk geen consequenties behoeft te hebben voor het oogmerk van de ontuchtige handelingen met een minderjarige. Tevens is in de toelichting verhelderd dat ook de poging strafbaar is. Het OM stemt in met de voorgestelde aanpassingen.

Op verzoek van het OM is de eerder voorgestelde verruiming tot het langs digitale weg corrumperen van een minderjarige (art. 248d Sr) geschrapt, andere strafbaarstellingen volstaan voor de aanpak van dergelijk strafwaardig gedrag. In plaats daarvan wordt voorgesteld de strafbaarstelling van het verleiden van een minderjarige tot ontucht (art. 248a Sr) te verruimen, zodat ook voor dit delict een oudere lokpuber kan worden ingezet. In de praktijk fungeert dit delict namelijk als ‘voorportaal’ van de grooming. Het OM heeft hierover aanvullend advies uitgebracht.

## 4. Afstemming

De reacties op de verschillende onderdelen van het advies van de Raad van State zijn afgestemd met de belanghebbenden, te weten de politie (onderzoek in geautomatiseerd werk) en het OM (onderzoek in geautomatiseerd werk en grooming) en besproken met de zittende magistratuur (identiteit geautomatiseerd werk en rechtsmacht).

Tevens zijn de reacties op de verschillende onderdelen van het advies van de Raad van State afgestemd met de belanghebbende ministeries, te weten het ministerie van BZK (grondrechten), van EZ (positie aanbieders) en van OC&W (bronbescherming journalisten).

++

# Nr. 014

**Van:** 10.2.e - BD/DRC/CV
**Aan:** 10.2.e - BD/DRC/CV
**Cc:** 10.2.e - BD/DRC/CV
**Onderwerp:** FW: Google - Impact WCCIII - Data 12 t/m 16 september?
**Datum:** donderdag 4 augustus 2016 15:55:34
**Bijlagen:** image002.png

---

Dit is nr 1 beantwoord jij hem? Groet simon

**Van:** 10.2.e [mailto:10.2.e @rvo.nl]
**Verzonden:** donderdag 4 augustus 2016 14:15
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Google - Impact WCCIII - Data 12 t/m 16 september?

Nav telefonisch contact met 10.2.e zonet, stuur ik jullie dit bericht: I.v.m. met andere gesprekken en mogelijke data daarvoor: Zou woensdag 14 september, in de ochtend een optie zijn?

Groet,

10.2.e


**Netherlands Foreign Investment Agency**
Ministry of Economic Affairs
T +31 10.2.g
M +31 10.2.e
E 10.2.e @nfia.nl
W www.investinholland.com
Prinses Beatrixlaan 2 | 2595 AL | The Hague | The Netherlands
P.O. Box 93144 | 2509 AC | The Hague | The Netherlands


**Van:** 10.2.e
**Verzonden:** dinsdag 2 augustus 2016 15:45
**Aan:** 10.2.e - BD/DRC/CV'; 10.2.e - BD/DRC/CV
**Onderwerp:** Google - Impact WCCIII - Data 12 t/m 16 september?

Beste 10.2.e en 10.2.e ,

Zoals eerder bericht (zie onderstaand), heeft Google gevraagd om een gesprek over o.a. de nieuwe Wet Computercriminaliteit III. Analyse van de impact daarvan op hun datacenter operatie is onderdeel van hun besluitvorming over mogelijke uitbreidingsinvesteringen.

Vanuit Google zijn de volgende personen aanwezig: 10.2.e (Parijs), 10.2.e , VS) en een vertegenwoordiger van Google Nederland. Zij zouden de week van 12 t/m 16 september naar Nederland kunnen afreizen. Kunnen jullie voor deze week aangeven op welke dagen / tijden jullie eventueel beschikbaar zouden zijn?

Wat betreft andere aanwezigen: Kunnen jullie een geschikte vertegenwoordiger uitnodigen van bijvoorbeeld het High Tech Crime team van de KLPD om een beeld te geven vanuit uitvoering? Ik zal zelf namens NFIA / Ministerie van Economische Zaken deelnemen.

Met dank en vriendelijke groet,

10.2.e


**Netherlands Foreign Investment Agency**
Ministry of Economic Affairs
T +31 10.2.g
M +31 10.2.e
E 10.2.e @nfia.nl
W www.investinholland.com
Prinses Beatrixlaan 2 | 2595 AL | The Hague | The Netherlands
P.O. Box 93144 | 2509 AC | The Hague | The Netherlands


**Van:** 10.2.e - BD/DRC/CV [mailto:10.2.e @minvenj.nl]
**Verzonden:** woensdag 6 juli 2016 15:08
**Aan:** 10.2.e ; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Google - Onderwerpen / vragen over WCIII

Dank we zien de uitnodiging tegemoet. Groet 10.2.e

**Van:** 10.2.e [mailto:10.2.e @rvo.nl]
**Verzonden:** woensdag 6 juli 2016 14:07
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
**Onderwerp:** Google - Onderwerpen / vragen over WCIII

Beste 10.2.e en 10.2.e ,

Kort geleden spraken wij elkaar over het verzoek van Google om een gesprek te organiseren over mogelijke impact van de WCCIII op een datacenter. Hierbij stuur ik u enkele bespreekpunten met het voorbehoud dat dit geen uitputtende lijst is, maar meer een indicatie. Google realiseert zich dat het wetsvoorstel zoals dit bekend is, mogelijk nog zal wijzigen. Niettemin gaan zij graag in gesprek over het huidige voorstel.

Onderwerpen / vragen:

• Kunnen de nieuwe hackbevoegdheden gebruikt worden om te proberen een datacenter te hacken? Zijn er situaties waarin dit denkbaar is?

• Zijn er andere manieren waarop deze wet impact kan hebben op een datacenter?

Het gaat hun uitdrukkelijk om een inschatting te maken van de praktische implicaties. Daarom lijkt het mij verstandig als bij de afspraak met Google een betrokkene vanuit een uitvoeringsorganisatie aanwezig is, om concreet te kunnen aangeven wat de huidige praktijk is en hoe die door de nieuwe wet naar verwachting zal veranderen (voor zover mogelijk binnen de grenzen voortvloeiende uit de vertrouwelijkheid van de betreffende opsporingsdienst).

Ik krijg binnenkort namen en datavoorstellen vanuit Google, en zal daarna weer contact opnemen.

Met dank en vriendelijke groet,

10.2.e

**Netherlands Foreign Investment Agency**
Ministry of Economic Affairs
T +31 10.2.g
M +31 10.2.e
E 10.2.e @nfia.nl
W www.investinholland.com
Prinses Beatrixlaan 2 | 2595 AL | The Hague | The Netherlands
P.O. Box 93144 | 2509 AC | The Hague | The Netherlands



---

verbonden aan het elektronisch verzenden van berichten.

Ministerie van Veiligheid en Justitie

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Security and Justice

De Rijksdienst voor Ondernemend Nederland (RVO.nl) stimuleert Duurzaam, Agrarisch, Innovatief en Internationaal ondernemen. RVO.nl is per 2014 ontstaan uit de fusie van Agentschap NL en Dienst Regelingen.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.
De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.
The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

# Nr. 015

**Van:** 10.2.e - BD/DRC/CV
**Aan:** 10.2.e - BD/DRC/CV 10.2.e - BD/DRC/CV
**Onderwerp:** FW: Google request
**Datum:** donderdag 4 augustus 2016 15:56:51

---

Dit is 5

-----Oorspronkelijk bericht-----
Van: 10.2.e [10.2.e @rvo nl]
Verzonden: vrijdag 1 juli 2016 11:23
Aan: 10.2.e - BD/DRC/CV
CC: 10.2.e - BD/DRC/CV
Onderwerp: Fwd: Google request

Beste 10.2.e ,

Dank voor het terugbellen nav mijn voice mail berichten.

Zoals ik al vertelde heb ik eerder deze week met 10.2.e gehad, cc.

Goed om te weten dat jullie bereid zijn tot een gesprek met Google. Zie onderstaand, hun verzoek.

Google Nederland stuurt mij de namen van personen door, een lijst specifieke vragen, en mogelijke data.

Groet,

10.2.e

[cid:image001.png@01D17ED8.302B6100]<http://www.investinholland.com/>

Netherlands Foreign Investment Agency
Ministry of Economic Affairs
T +31 10.2.g <tel:+3110.2.g > M +31 10.2.e <tel:+3110.2.g > E 10.2.e @nfia.nl<10.2.e @nfia nl> W www.investinholland.com<http://www.investinholland.com/>
Prinses Beatrixlaan 2 | 2595 AL | The Hague | The Netherlands P.O. Box 93144 | 2509 AC | The Hague | The Netherlands

Begin doorgestuurd bericht:

Van: 10.2.e <10.2.e @google.com<10.2.e @google.com>>
Datum: 23 juni 2016 15:19:55 CEST
Aan: "10.2.e @nfia nl<10.2.e @nfia.nl>" 10.2.e @nfia nl<10.2.e @nfia.nl>>
Kopie: 10.2.e <10.2.e @google.com<10.2.e @google.com>>, 10.2.e 10.2.e @google.com<10.2.e @google.com>>, 10.2.e <10.2.e @google.com10.2.e @google.com>>
Onderwerp: Google request

Dear 10.2.e

Thanks for getting back to me on the phone. As agreed an e-mail with our request to you.

10.1.C we (the NL policy team for Google) are receiving questions from our headquarters on two specific bills that could have consequences for data centers. The two bills are:
- Wet Computercriminaliteit III (WCIII)

- Wet op de Inlichtingen- en Veiligheidsdiensten (WIV)

10.1.C

Therefore we are requesting a meeting with representatives of the ministries that are drafting the two mentioned laws, i.e. Ministry of Home Affairs on the WIV and Ministry of Security and Justice on the WCIII. 10.1.C

Most important subject in the meeting would be the consequences for data centers, both legal and practical.
10.1.C

To conclude, I will be leaving Google per July 1st, therefore 10.2.e (cc.) and later 10.2.e (cc.) will take back this project. If you can 'reply all' to this e-mail we can make sure that the right person picks this up.
[https://ssl.gstatic.com/ui/v1/icons/mail/images/cleardot.gif]

Thanks and best,

10.2.e

# Nr. 016

**Van:** 10.2.e @kpn.com
**Aan:** 10.2.e - BD/DRC/CV
**Cc:** 10.2.e @office.ziggo.nl; 10.2.e @vodafone.com; 10.2.e @office.ziggo.nl; 10.2.e - BD/DGPenV/PVC/MCA
**Onderwerp:** RE: Uitnodiging workshop IViR rapport 'Geheime surveillance en opsporing' – vrijdag 18/11, Den Haag
**Datum:** donderdag 17 november 2016 08:10:44
**Bijlagen:** Geheime surveillance en opsporing 1.2 - org.pdf

---

Beste 10.2.e,
Dank voor jouw aanmelding voor de workshop morgen. In afstemming met 10.2.e bijgevoegd het, morgen te bespreken, rapport. Bijgevoegd exemplaar betreft laatste concept versie. Na de workshop morgen zal de definitieve versie worden samengesteld. Details over verdere tijdlijn en beschikbaarheid van de definitieve versie zal morgen aan de orde zijn.
De nu beschikbare versie is voor persoonlijk gebruik in de voorbereiding van de bijeenkomst morgen.
Zie uit naar de bijeenkomst morgen.
Met vriendelijke groet,
10.2.e, 10.2.e, 10.2.e en 10.2.e

---

**Van:** 10.2.e
**Verzonden:** woensdag 9 november 2016 7:44
**Aan:** 10.2.e @minvenj.nl
**CC:** 10.2.e '; 10.2.e 10.2.e @vodafone.com'; 10.2.e 10.2.e @office.ziggo.nl)
**Onderwerp:** Uitnodiging workshop IViR rapport 'Geheime surveillance en opsporing' – vrijdag 18/11, Den Haag
Beste 10.2.e,
Effectief toezicht en transparantie zijn centrale elementen bij het vormgeven en evalueren van de wettelijke waarborgen rond digitale geheime surveillance door nationale inlichtingen- en veiligheidsdiensten. De eerdere IViR-studie 'Ten standards for oversight and transparency of national intelligence services' formuleert tien richtsnoeren die dit verder uitwerken.
Door middel van het uitwerken van een quickscan heeft een consortium bestaande uit KPN, Vodafone en Ziggo het IViR gevraagd om te onderzoeken in hoeverre deze tien richtsnoeren ook van toepassing zijn op geheime surveillance in het kader van de opsporing van strafbare feiten. Het belang van het onderzoek, dat is uitgevoerd onder leiding van 10.2.e, wordt ingegeven door het feit dat in een aantal recente wetsvoorstellen nieuwe bevoegdheden voor het verzamelen en verwerken van persoonsgegevens worden geïntroduceerd. Het wetsvoorstel Computercriminaliteit III is een typisch voorbeeld van deze ontwikkeling en wordt daarom gebruikt om te illustreren hoe de geformuleerde richtsnoeren toegepast kunnen worden.
In een workshop sessie willen wij je aan de hand van een presentatie door de onderzoekers graag als eerste inzicht geven in de resultaten van het rapport en willen we graag de resultaten met de genodigden bediscussiëren. We hopen dan ook zeer op jouw deelname. Het rapport wordt je na bevestiging toegezonden.
**Workshop IViR rapport 'Geheime surveillance en opsporing'**
Tijd**: Vrijdag 18 november, van 10:00 – 12:00**
Locatie**: NL Kabel, Lange Voorhout 90, Den Haag**
Zou je je deelname kunnen bevestigen via een email aan 10.2.e @office.ziggo.nl ?
Bij voorbaat dank en graag tot de 18e.
Met vriendelijke groet,
10.2.e, 10.2.e, 10.2.e en 10.2.e

ECP

# Nr. 017

Platform voor de InformatieSamenleving

## Notulen Platform Internetveiligheid

| | | |
|---|---|---|
| **Vergadering**: | | Platform Internetveiligheid |
| **Datum** | : | Dinsdag 13 december 2016 |
| **Tijd** | : | 12:30-14.00 uur |
| **Plaats** | : | Sociëteit de Witte, Plein 24 Den Haag<br>Littéraire Zaal |

1. **Opening vergadering**
   - Vaststellen verslag

2. **Mededelingen**
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte
   - Buiten reikwijdte

- Buiten reikwijdte
- Buiten reikwijdte
- Buiten reikwijdte

3. **Toelichting conclusies rapport 'Geheime surveillance en opsporing' door** 10.2.e **(KPN)**

Het Instituut voor informatierecht heeft het rapport 'geheime surveillance en opsporing – richtsnoeren voor de inrichting van wetgeving' geschreven. De richtsnoeren die hier worden gegeven kunnen worde toegepast op bestaande wettelijke voorzieningen m.b.t. toezicht en transparantie. Vervolg zal worden gegeven bijvoorbeeld in de vorm van een lijst van aandachtspunten i.s.m. Ziggo en Vodafone.

4. **Digital Trust Center door** 10.2.e **(Nederland ICT)**

Buiten reikwijdte

Buiten reikwijdte

5. **CC3:**

Het grootste probleem is het toezichtsvraagstuk, echter ten behoeve van transparantie is het debat positief. Het decryptie bevel is weggevallen, gevoel is dat we daar nog iets mee moeten doen. Zonder de encryptie te verzwakken hier wel iets mee doen; decryptie is namelijk belangrijk voor opsporing. Gaat om gerichte situaties (geen sleepnetten etc.) waar in samenwerking dit mogelijk zou moeten worden.

Er is sprake van een complexe situatie als het aankomt op de beschikking hebben van bepaalde achterdeuren (kwetsbaarheden) van verschillende actoren. Die maakt de discussie zo ingewikkeld dat de oplossing niet zomaar in zicht is. Kiezen voor simpele gelaagdheid kan uitkomst bieden; beveiliging vóór opsporings- en inlichtingsbelang. Veiligheid van iedereen incl. gegevensbescherming & bescherming van de persoonlijke levenssfeer. Wanneer zwakheid in encryptiesysteem wordt detecteert is stap een het melden en zorgen oplossing, stap twee is gebruik maken van de zwakheid als opsporingsdienst. D.m.v. stellen van prioriteiten maak je het minder complex.

Er is behoefte om dit fundamentele vraagstuk in een bredere context op te pakken en de discussie te voeren met de vier vragers voor kwetsbaarheden. Het doel is tot bijvoorbeeld een aanbeveling te komen. Voorstel is een strategische sessie voorafgaande aan de verkiezingen met vijf belangendragers; politie, nfi, aivd, en defensie en industrie.

**Oproep aan het PIV voor relevante namen voor een strategische sessie m.b.t. dit onderwerp bij:**

- **Politie**
- **NFI**
- **AIVD**
- **Defensie**

6. **WIV**

Buiten reikwijdte

## 7. Werkplan 2017

Buiten reikwijdte

*Rondvraag*

Buiten reikwijdte