NEDERLAND ICT

Minister van Veiligheid & Justitie, de heer I.W. Opstelten
Ministerie van Veiligheid & Justitie
Postbus 20301
2500 EH DEN HAAG

Woerden, 1 juli 2013

Betreft : reactie Nederland ICT op consultatie wetsvoorstel computercriminaliteit III
Kenmerk : 35490/BP

Geachte heer Opstelten,

De inzet van ICT draagt bij aan 60 procent van de economische groei in Nederland. 70 procent van alle innovaties is ICT-gerelateerd. Met een toenemende afhankelijkheid in de samenleving van ICT, een tegelijk toenemend aantal digitale dreigingen en de praktijk waarin cybercriminelen kwetsbaarheden sneller weten uit te buiten, moet de samenleving investeren in de digitale veiligheid van deze voorzieningen. Hierdoor blijft er vertrouwen in ICT en kunnen we blijvend profiteren van de toegevoegde waarde van ICT.

Dit vraagt naast allerlei preventieve maatregelen en het tijdig opmerken van criminaliteit ook een adequaat juridisch kader om cybercriminaliteit te bestrijden. De pakkans voor deze criminelen is momenteel veel te laag, waardoor crimineel gedrag niet aangepakt wordt. Nederland ICT ondersteunt daarom ook de zoektocht van het kabinet naar passende (juridische) middelen en bevoegdheden om tegenwicht te bieden aan cybercriminaliteit.

Voor de consultatie van het wetsvoorstel computercriminaliteit III richt Nederland ICT zich primair op twee onderdelen van het wetsvoorstel:

1. Voorstel voor (heimelijk) onderzoek in een geautomatiseerd werk ingeval van verdenking van ernstig strafbaar feit.
2. Herziening van de bestaande regeling van artikel 54a Wetboek van Strafrecht over het ontoegankelijk maken van gegevens op het internet.

1. Voorstel voor nieuwe bevoegdheid om een geautomatiseerd werk (heimelijk) te onderzoeken

Nederland ICT heeft ernstige twijfels bij de in te stellen nieuwe bevoegdheid om op afstand heimelijk binnen te dringen in een geautomatiseerd werk ten behoeve van opsporing van ernstig strafbare feiten. Hierbij gaat het Nederland ICT voornamelijk om de neveneffecten en precedentwerking die deze nieuwe bevoegdheid kan hebben. De twijfels heeft Nederland ICT hieronder tot uiting gebracht in enkele opmerkingen en vragen.

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@nederlandict.nl
www.nederlandict.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

Locatie Den Haag:
Caballero Fabriek, unit 97
Saturnusstraat 60

In algemene zin vreest Nederland ICT voor de effecten die het mogen binnendringen van opsporingsdiensten heeft op het vertrouwen in ICT. Burgers en bedrijven zien hun computer(systemen) als privéomgeving. Wanneer de overheid hierop inbreuk kan maken, kan dit het vertrouwen in ICT remmen en daarmee ook het gebruik van ICT. Dit kan negatieve gevolgen hebben voor de bijdrage van ICT en het internet aan economische groei.

Neveneffecten
Voor wat betreft de neveneffecten heeft Nederland ICT een aantal vragen:

- Wat is de **afbakening** van een geautomatiseerd werk? Juist in een wereld waarin steeds meer ICT aan het internet is verbonden, en deze ICT in steeds maar apparaten van dagelijks gebruik is verwerkt, komt de vraag op of er een nadere afbakening dient te zijn voor welk type werken deze bevoegdheid in het leven wordt geroepen. De vraag is of de slimme energiemeter, het digitale hardloophorloge, de TV settopbox en de draadloos met internet verbonden boordcomputer van een auto ook relevante werken zijn die onder de definitie zouden vallen. Dit geldt temeer daar de definitie van "geautomatiseerde werk" in de jurisprudentie in beperkende termen is gedefinieerd en deze definitie middels voorgenomen aanpassing van artikel 80sexies weer wordt verruimd.

  Nederland ICT vraagt zich in combinatie met de eerdere opmerking af of in de afbakening geen uitsluiting moet zijn opgenomen voor het moment wanneer er een vermoeden is dat het te onderzoeken geautomatiseerd werk een werk betreft dat in gebruik is bij een enkele natuurlijke persoon voor "huishoudelijk gebruik".

- Waar er behoefte is aan betere opsporing en vervolging van cybercriminaliteit regelt dit wetsvoorstel ook de digitale opsporing voor de 'traditionele' criminaliteit. Nederland ICT vraagt zich af of daarmee niet twee **verschillende doelen** worden beoogd, waar het voor Nederland in de kern juist gaat om het veiliger maken van het internet door slimmer op te treden van opsporingsdiensten. Zal de verbreding er niet toe leiden dat de schaarse technische capaciteit van de opsporing teveel verwatert door het beroep dat op deze capaciteit wordt gedaan vanuit de opsporing van 'traditionele' criminaliteit?

- Een derde vraag betreft de **impact** die onderzoek van opsporingsambtenaren heeft op het werk waarop wordt binnengedrongen. Door het onderzoeken en het mogelijk achterlaten van speciale software kunnen veranderingen in het werk ontstaan en kan zelfs het systeem ontregeld raken. Zoals vaak wordt aangehaald dat ethische hackers onbedoeld schade aan kunnen richten, zo kan dit ook voor 'hackende' opsporingsambtenaren gelden. Zeker in combinatie met de eerste vraag over de afbakening van binnen te treden werken, is de vraag of de impact van binnendringen vooraf ook maar enigszins te voorzien en te overzien is, zeker wanneer niet meteen bekend is wat de omvang en functie van het werk is dat achter het betreffende IP-adres schuilgaat. Dit speelt des te sterker wanneer deze werken gebaseerd zijn op intellectuele eigendommen van producenten, die zij confidentieel wensen te houden.

- Nederland ICT is ook benieuwd hoe opsporingsambtenaren handelen wanneer ze een kwetsbaarheid in een systeem vinden, vooral wanneer dit een bredere kwetsbaarheid is in een beveiligingstechnologie, in software of in de firmware op apparaten. Het zijn deze kwetsbaarheden die ambtenaren toegang verschaffen tot systemen. Tegelijk heeft het kabinet zich ook tot doel gesteld om de beveiliging van systemen en software te vergroten.

  In de concept Memorie van Toelichting merkt het kabinet op dat systemen dikwijls standaard zijn ingesteld op versleutelde vormen van communicatie en dat gebruikers, zonder dit zelf na te streven, steeds beter zijn beveiligd tegen afluisteren. Nederland ICT ziet in de opmerking een bevestiging dat hard- en software steeds beter *by default* beveiligd zijn.

  Tegelijk heeft het kabinet zich ten doel gesteld om kwetsbaarheden in ICT sneller op te merken en verholpen te krijgen door hierover kennis en informatie te delen met het Nationaal Cyber Security Centrum en door de bevordering van responsible disclosure beleid door middel van de eerder dit jaar gepubliceerde leidraad. Dit roept de vraag op of opsporingsdiensten **direct melding maken bij leveranciers van de gevonden kwetsbaarheid** (eventueel geanonimiseerd door tussenkomst van het NCSC) wanneer bij het zoeken naar een manier om een geautomatiseerd werk binnen te dringen er een kwetsbaarheid is ontdekt in het systeem. Nederland ICT is daarbij ook benieuwd wat het kabinet verwacht hoe organisaties omgaan met de meldplicht voor cyber security incidenten of datalekken. Zal in het kader van security breach of data breach notification melding gemaakt moeten worden van het binnentreden door opsporingsdiensten?

- Een vijfde vraag betreft de **aansprakelijkheid** voor de schade die mogelijk wordt veroorzaakt door het handelen van opsporingsambtenaren. Op de systemen van de verdachte kan schade worden veroorzaakt, bewust door het ontoegankelijk maken van gegevens of onbewust door de neveneffecten van het handelen. Mogelijk kan de schade zich ook uitstrekken tot andere personen die van hetzelfde geautomatiseerde werk gebruik maken, maar niet verdachte zijn, of tot bedrijven die bijvoorbeeld een cloudcomputing dienst aanbieden waarvan verdachte gebruik maakt. Hoe gaat de minister om met de compensatie van geleden schade?

Cloud computing

Nederland ICT heeft ernstige twijfels bij de redenatie achter de nieuwe bevoegdheden waar het cloudcomputing diensten betreft. De lijn van argumentatie over de noodzaak en omstandigheden waarvoor deze bevoegdheden in geval van gegevens in de 'cloud' van toepassing zou moeten zijn, lijkt erop te wijzen dat de minister deze bevoegdheid wil gebruiken zo gauw er sprake is van cloudcomputing diensten. Het benoemen van 'bulletproof hosting providers' in de tekst roept de gedachte op dat de bevoegdheid alleen bij deze vaak illegaal handelende bedrijven zal worden gebruikt. Dat blijkt echter in de rest van de tekst uit niets en dat baart Nederland ICT zorgen.

Het overgrote deel van de aanbieders van communicatie-, hosting- en cloud computingdiensten werkt mee aan een strafrechtelijk onderzoek wanneer de Officier van Justitie, gemachtigd door de rechter-commissaris, hiertoe beveelt. Gezien de vertrekkende gevolgen voor de veiligheid van de systemen en de inbreuk op de privacy van gebruikers stelt Nederland ICT zich op de positie dat informatieverzoeken louter en alleen via een door de rechter gemachtigd bevel kunnen worden

gedaan en dat het (al dan niet heimelijk) installeren van apparatuur op netwerken en systemen en/of opzetten van programma's die toegang geven tot de digitale omgeving van aanbieders geen begaanbare route is. Niet alleen kan de inzet van de voorgenomen bevoegdheid neveneffecten opleveren in het netwerk van de aanbieder, ook kan het aanbieders in een spagaat brengen richting de eigen klanten en gebruikers. Hierdoor heeft het indirect ook negatieve effecten op de reputatie van bedrijven wanneer overheden kunnen binnendringen op netwerken.

In algemene zin vraagt Nederland ICT zich af hoe de bevoegdheid in relatie tot cloudcomputing diensten zich verhoudt tot de jurisdictie in andere landen, indien de servers buiten Nederland staan.

Onderzoek bij aanbieder als cyber security incident
Wanneer opsporingsambtenaren toegang hebben verschaft tot het netwerk van de aanbieder is er sprake van een cyber security incident. Ten eerste zal de aanbieder de indringer van zijn netwerk proberen te weren, mogelijk door hulp van (collega) opsporingsinstanties in te schakelen. Ten tweede dient de aanbieder, veelal op grond van contractuele verplichtingen, melding te maken bij zijn klanten van een inbreuk op de beveiliging. Dit kan effect hebben op de reputatie van de betreffende aanbieder bij zijn klanten. Tevens kan dit leiden tot directe operationele kosten door inzet van derden om het beveiligingsincident tegen te gaan en door het ondersteunen van klanten. Ook zou dit kunnen leiden tot het activeren van malus clausules in contracten waardoor de leverancier een klant dient te compenseren.

Precedent
Nederland ICT is positief over de keuze van het kabinet om de inzet van de voorgestelde bevoegdheden eerst ter toetsing voor te leggen aan de Centrale Toetsingscommissie (CTC). Van belang is dat de CTC voldoende onderlegd is om de voorgenomen inzet en de impact ervan op systemen daadwerkelijk te toetsen. Het gaat om specialistisch werk en inzet van nieuwe bevoegdheden, waarvoor op alle niveaus in de organisatie kennis aanwezig dient te zijn om de juiste besluiten te nemen waarbij de impact goed overzien kan worden. Deze kennis moet aanwezig zijn voordat de nieuwe bevoegdheid in werking treedt.

Nederland ICT vraagt zich af of deze kennis tijdig kan worden bijgebracht onder de betrokken opsporingsambtenaren, Officieren van Justitie en leden van de CTC. De afweging aan de kant van het Openbaar Ministerie vraagt tegelijk om een inhoudelijk tegenwicht aan de kant van de rechterlijke macht. Nederland ICT vraagt zich af of van de rechter-commissaris wel voldoende tegenwicht verwacht mag worden tegen een voorbereid bevel van het Openbaar Ministerie. Kortom, zal de toets van de rechter-commissaris in de praktijk niet teveel een papieren exercitie worden wegens gebrek aan specialistische kennis?

De drempel van een toetsing door de CTC zou er ook toe moeten leiden dat de inzet van de bevoegdheden beperkt blijft tot wanneer deze echt noodzakelijk is. Nederland ICT is benieuwd in hoeveel gevallen de minister verwacht gebruik te gaan maken van deze bevoegdheden. Daarbij zou Nederland ICT voorstander zijn van een jaarlijkse melding van het aantal verzoeken, hun aard en bij welke bedrijven deze zijn gedaan. Dit is essentieel zodat bedrijven hun gebruikers achteraf kunnen informeren. Voor het vertrouwen in dit steeds belangrijker wordende deel van onze economie is transparantie een onmisbaar element.

Nederland ICT vindt het belangrijk dat opsporingsambtenaren eerst alles doen binnen de bestaande bevoegdheden, voordat ze gebruik maken van de nieuwe bevoegdheid. Het zou wat Nederland ICT betreft moeten gaan om bevoegdheden als ultimum remedium. Nederland ICT vreest wel voor een glijdende schaal, waarbij ondanks de benodigde toetsing door de CTC er toch sneller gekozen zal worden voor de inzet van deze speciale bevoegdheid omdat hierdoor minder afhankelijkheid bestaat van derden, bijv. aanbieders van communicatie-, hosting- en/of clouddiensten. Het voorstel ontbeert op dit moment een juridisch kader om te toetsen of de bevoegdheid wel of niet als ultimum remedium zal worden ingezet.

Internationaal precedent

Het grootste risico ziet Nederland ICT in het precedent dat hiermee ook internationaal wordt geschapen. Nederland kan goede waarborgen in zijn nationale wetgeving hebben geregeld. Andere staten kunnen een soortgelijke bevoegdheid in het leven roepen, voorzien van minder voor Nederland van belang zijnde waarborgen, waarbij ook zij zich kunnen beroepen op de eigen wetgeving. De voorstellen van het kabinet scheppen ook op een ander punt een precedent. Zij lijken inbreuk te maken op - in ieder geval - twee punten die gemeengoed zijn in het internationaal recht: het principieel rechtsbeginsel van soevereiniteit van staten en de rechten van de burgers die daar wonen.

Een internationaalrechtelijk kader voor voorgenomen bevoegdheden ontbreekt. In dat verband vraagt Nederland ICT in het bijzonder een beschouwing over de verhouding van de in het voorontwerp vastgelegde bevoegdheden en het bepaalde in het Cybercrime Verdrag van Budapest, waarbij ook Nederland partij is. In het bijzonder vraagt Nederland ICT uw aandacht voor de verhouding met artikel 19 van dit Verdrag.

Zoals ook in de concept Memorie van Toelichting staat beschreven konden opstellers van het Cybercrime Verdrag het niet eens worden over de internationale samenwerking bij het bestrijden van cybercrime. Dit toont wat Nederland ICT betreft juist aan dat internationale afspraken nodig zijn en dit niet vraagt om een unilaterale bevoegdheid. Tevens gaat de nieuwe bevoegdheid om buiten het huidige systeem voor samenwerking op (cyber)crime, namelijk die van Onderlinge Rechtsbijstand Overeenkomsten (het zogenaamde MLAT-systeem).

Nederland is een digital gateway naar Europa, heeft een van de beste telecominfrastructuren in de wereld en daarmee een zeer hoge bedrijvigheid in datacenters en hostingproviders. Juist Nederland heeft hiermee ook een goede reden om haar eigen bedrijven te willen beschermen tegen onderzoeken van buitenlandse opsporingsdiensten op Nederlandse servers. Het introduceren van dergelijke bevoegdheden door Nederland creëert een internationale precedent dat vooral ook Nederlandse bedrijven kan schaden. Nederland ICT heeft daarbij al concrete voorbeelden ontvangen van bedrijven (in de klantenkring van aangesloten ICT-bedrijven) die dit type bevoegdheden in hun afweging voor het te kiezen vestigingsland meenemen.

Nederland ICT is vanuit deze optiek tegen de nieuwe bevoegdheid tot binnendringen van geautomatiseerde werken. Als het kabinet de bevoegdheid doorzet, ziet Nederland ICT graag nader toegelicht hoe het kabinet de afweging maakt tussen het opsporingsbelang enerzijds en de economische impact en het Nederlandse vestigingsklimaat anderzijds.

Oplossingsrichting
Wat Nederland ICT betreft is het van belang dat in plaats van aan te sturen op nationale bevoegdheden, er een deugdelijk internationaalrechtelijk kader is met het oog op de bestrijding van cybercriminaliteit dat ook verdere afspraken regelt over verregaande opsporingsbevoegdheden.

Nederland ICT kan zich daarnaast indenken dat het versterken van het huidige MLAT-systeem in de tussentijd een prioriteit wordt van het kabinet. Bovenal is van belang op te merken dat dit systeem op dit moment de meeste waarborgen voor bedrijfsleven en burgers biedt dat er zorgvuldig met de rechten en verantwoordelijkheden van de belanghebbenden wordt omgegaan.

Nederland ICT vindt het verder van groot belang dat opsporingsdiensten de door hen gevonden kwetsbaarheden in software direct melden bij het NCSC, zodat het NCSC dit (anoniem) kan doormelden aan de betreffende leverancier.

Cybercriminaliteit treft grote en kleine bedrijven. Het wetsvoorstel lijkt vooral betrekking te hebben op de high-end zaken. Nederland ICT is benieuwd hoe het kabinet de kleine ondernemingen in Nederland de mogelijkheid wil bieden om melding te maken van cybercriminaliteit of verdachte situaties en hoe opsporingsdiensten deze informatie kunnen aggregeren tot high-end zaken.

2. Herziening van de bestaande regeling van artikel 54a Wetboek van Strafrecht over het ontoegankelijk maken van gegevens.

Het voorliggende wetsvoorstel behelst ook het voorstel om de bestaande bepaling in artikel 54a Wetboek van Strafrecht over het bevel van de Officier van Justitie voor het ontoegankelijk maken van gegevens op internet over te hevelen naar het Wetboek van Strafvordering. Waar dit artikel de Notice-and-Take-Down bevoegdheid in de wet regelt, leidt de voorgestelde wijziging niet direct tot verruiming van de bevoegdheden. Nederland ICT heeft ook in een eerdere consultatie gereageerd op het toenmalige voorstel. Wij zijn dan ook tevreden dat het door Nederland ICT aangedragen bezwaar dat het bevel van de Officier niet van een machtiging hoeft te worden voorzien in dit wetsvoorstel een plek heeft gekregen.

Ook het toenmalige voorstel van de eigen rol die de aanbieder in het vorige wetsvoorstel werd toebedeeld op het inschatten of materiaal op het internet strafbaar is, is uit dit voorstel gehaald. Nederland ICT is het ook van harte eens met de aanpassingen die hierover zijn gemaakt. Ook het verwijderen van de bepaling die het opleggen van een dwangsom mogelijk maakt, juicht Nederland ICT toe.

Door het wegnemen van deze eerdere bezwaarpunten is Nederland ICT in grote lijnen positief over het wetsvoorstel zoals dit nu is voorgelegd. Wel blijft Nederland ICT de vraag houden in welke gevallen de bepaling zal worden ingezet in de praktijk. De huidige praktijk van zelfregulering met de Notice-and-Take-Down procedure blijkt immers goed werkbaar. In deze procedure is door aanbieders al afgesproken hoe te handelen bij een melding van strafbare of onrechtmatige inhoud op het internet. Het ministerie van Veiligheid & Justitie heeft met enige regelmaat overleg met marktpartijen hoe om te gaan met deze materie.

Tevens is Nederland ICT benieuwd hoe hetgeen geregeld in het voorgestelde artikel 54a Wetboek van Strafrecht en artikel 125p Wetboek van Strafvordering zich verhoudt tot hetgeen bepaald in artikel 7.4a Telecommunicatiewet. In deze laatstgenoemde wet is de bepaling opgenomen dat aanbieders geen diensten of toepassingen op het internet mogen belemmeren of vertragen. In lid d van dit artikel wordt hierop een uitzondering gemaakt voor de uitvoering van een wettelijk voorschrift of rechterlijk bevel. Om te voorkomen dat aanbieders van elektronische communicatiediensten vast komen te zitten tussen twee tegenstrijdige verplichtingen van beide hiervoor genoemde wetten, vraagt Nederland ICT hierover een nadere duiding in de Memorie van Toelichting. Nederland ICT zou graag zien dat in de Memorie duidelijk wordt of een bevel van de Officier van Justitie, gemachtigd door de rechter-commissaris, zoals voorgesteld in het voorliggende wetsvoorstel gelijk staat aan een rechterlijk bevel in artikel 7.4a, lid d van de Telecommunicatiewet.

3. Verdere overweging: wijziging artikel 139f Wetboek van Strafrecht

Nederland ICT is daarnaast benieuwd hoe de aanpassing van artikel 139f Wetboek van Strafrecht met invoeging van lid 2 zich verhoudt met het door het kabinet gestimuleerde beleid voor responsible disclosure. Bij responsible disclosure meldt een derde die een kwetsbaarheid heeft gevonden op het systeem van een organisatie zich bij die organisatie en maakt geen misbruik van de kwetsbaarheid en publiceert niet over deze kwetsbaarheid totdat de kwetsbaarheid is verholpen.

Nederland ICT vraagt zich af of lid 2 er niet toe zal leiden dat hackers die menen dat het in het algemeen belang is om kwetsbaarheden in een ICT-systeem aan te tonen en dit bekend te maken in het publiek, zich op dit lid zullen beroepen om zich aan het responsible disclosure beleid te kunnen onttrekken. Nederland ICT is benieuwd of een nadere duiding hiervan in de Memorie van Toelichting duidelijkheid kan scheppen.

Afsluiting

Nederland ICT bedankt u voor de mogelijkheid om te reageren op het voorontwerp voor het wetsvoorstel computercriminaliteit III. Als u naar aanleiding van deze opmerkingen vragen heeft, ben ik natuurlijk graag bereid een nadere toelichting te geven.

Met vriendelijke groet,
Nederland ICT

Peter van Schelven
Algemeen directeur a.i.

In afschrift aan:
de minister van Economische Zaken, de heer H.G.J. Kamp