Nederlands Juristen Comité voor de Mensenrechten
Dutch section of the International Commission of Jurists

Ministerie van Veiligheid en Justitie
T.a.v. de Minister van Veiligheid en Justitie
Postbus 20301
2500 EH Den Haag

Leiden, 28 juni 2013

Betreft: consultatie conceptwetsvoorstel versterking bestrijding computercriminaliteit

Excellentie,

Op 13 mei 2013 werden het conceptwetsvoorstel versterking bestrijding computercriminaliteit en de bijbehorende memorie van toelichting gepubliceerd. Het doel van het wetsvoorstel is om opsporingsbevoegdheden in evenwicht te brengen met de stand van de technologie. Het Nederlands Juristen Comité voor de Mensenrechten (NJCM) wil graag gebruik maken van de door u opengestelde internetconsultatie. Wij hebben onderzocht of het wetsvoorstel ook in evenwicht is met het recht op een eerlijk proces, de vrijheid van meningsuiting en met de bescherming die de overheid aan de privacy hoort te geven. Hieronder bespreken wij onze zienswijze op een vijftal onderwerpen uit het wetsvoorstel.

1. (Technische) noodzaak en effectiviteit hacken

De reden om de opsporingsbevoegdheden ten aanzien van computercriminaliteit uit te breiden is volgens de concept-memorie van toelichting (MvT) erin gelegen dat bestaande opsporingsbevoegdheden in toenemende mate tekortschieten om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen. Hoewel het NJCM zich realiseert dat de in hoog tempo voortschrijdende ontwikkelingen op het gebied van ICT een aanpassing van de opsporingsbevoegdheden noodzakelijk maken, acht zij het van belang kritisch te kijken naar de (technische) noodzaak en de te verwachten effectiviteit van de doorzoeking ter vastlegging van gegevens en onderzoek in een geautomatiseerd werk.

Er zijn meerdere manieren om een geautomatiseerd werk binnen te dringen. Opsporingsambtenaren gaan doorgaans op zoek naar kwetsbaarheden in software. Zo kunnen zij onbedoeld baat krijgen bij het achterhouden van systeemkwetsbaarheden. Dit staat haaks op de algehele maatschappelijke wenselijkheid om gezamenlijk informatiesystemen veiliger te maken. Kwetsbaarheden zouden door opsporingsinstanties moeten worden gemeld, in plaats van enkel ten behoeve van de opsporing te worden gebruikt. Het binnendringen in een geautomatiseerd werk kan daarnaast ongewenste gevolgen hebben. Zo kan het systeem van de verdachte door het binnendringen crashen en onbruikbaar worden. Dit kan vooraf moeilijk worden uitgesloten. Het NJCM zou graag verduidelijkt willen zien hoe het wetsvoorstel deze problemen kan ondervangen.

Steenschuur 25
2311 ES Leiden, The Netherlands
Postal address: p.o. box 9520
2300 RA Leiden, The Netherlands
Telephone +31 (0)71 52 777 48
www.njcm.nl
ING 3540940
KvK Leiden 40445896

Het voorstel maakt het mogelijk voor de opsporing om heimelijk software te installeren op een geautomatiseerd werk van de verdachte. In de Duitse 'Staatstrojaner'-discussie is gebleken dat staatstrojans extra kwetsbaarheden in het systeem kunnen introduceren.[1] Naast het feit dat de verdachte extra kwetsbaar gemaakt wordt, kunnen er ook vraagtekens worden geplaatst bij de integriteit van het bewijsmateriaal. Ook bestaat de mogelijkheid dat de verdachte de staatstrojan detecteert en daarna bewijsmateriaal gaat wissen.

Daarnaast brengt het voornemen van de minister om de acties van de software van opsporingsdiensten op het geautomatiseerde werk van de verdachte te 'loggen' uitvoeringsproblemen met zich mee. Op het moment dat het geautomatiseerd werk van de verdachte offline is, heeft deze verdachte (of een kwaadwillende derde) alle tijd om de logs van de opsporingsambtenaar te vervalsen.

Ten aanzien van al deze punten beveelt het NJCM de minister aan om duidelijker te maken hoe de betreffende problemen kunnen worden geadresseerd.

Ten aanzien van het ontoegankelijk maken van gegevens wordt in paragraaf 2.1 van de MvT de indruk gewekt dat ook de AIVD en de MIVD deze bevoegdheid hebben. Dit is onjuist. Artikel 24 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 geeft deze diensten enkel de mogelijkheid om binnen te dringen in een geautomatiseerd werk en de gegevens die daar zijn opgeslagen of verwerkt over te nemen.

2. Privacyvragen en –waarborgen hacken

2.1 Reikwijdte
Het wetsvoorstel is blijkens de titel gericht op de verbetering en versterking van de opsporing en vervolging van computercriminaliteit. Toch heeft de minister ervoor gekozen om de nieuwe opsporingsbevoegdheden niet alleen toe te staan bij een verdenking van cybercriminaliteit, maar ook bij de verdenking van andere strafbare feiten waarvoor voorlopige hechtenis voorzien is (artikel 67, eerste lid, Sv). Dit wekt verwarring. In wezen wordt de hackbevoegdheid zoals de minister deze voorstelt dan een algemeen opsporingsmiddel en is het toepassingsbereik vergelijkbaar met dat van bijvoorbeeld de afluisterbevoegdheid. Het NJCM vindt dit ruime toepassingsbereik gelet op de ernst van de inbreuk op de privacy van betrokkene(n) onwenselijk. Ook technische experts benadrukken dat de inzet van de hackbevoegdheid geen algemeen opsporingsmiddel moet worden en dat in dit opzicht het voorstel van de minister dus te breed is geformuleerd.[2] Het NJCM stelt voor om in het wetsvoorstel een limitatieve opsomming op te nemen van de misdrijven waartegen de nieuwe bevoegdheden ingezet mogen worden.

2.2 Privacyvragen hacken
De mate van inbreuk op de privacy die de hackbevoegdheid maakt hangt af van de gegevens waartoe toegang verkregen kan worden. Met een hack op een geautomatiseerd werk kan niet alleen toegang worden verkregen tot het e-mailverkeer van de verdachte, maar ook bijvoorbeeld op diens foto's, documenten, agenda of betalingsverkeer. In dit opzicht is de potentiële inbreuk die een hack op de privacy maakt vele malen groter dan bijvoorbeeld de

[1] Zie o.a. http://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner.
[2] Zie o.a. B. Jabobs, 'Policeware', *NJB* 2012, p. 2761- 2764.

inbreuk van een telefoontap. Ook de privacy van anderen die het geautomatiseerde werk gebruiken, zoals de huisgenoten van de verdachte, kan in het geding zijn. Vanuit het oogpunt van de privacy moet worden voorkomen dat de hackbevoegdheid zonder onderscheid toegang geeft tot al deze gegevens.
Daarom dient in de verkennende fase zoals omschreven in paragraaf 2.5.1 van de MvT niet alleen aandacht te zijn voor de technische dimensie van het onderzoek. Ook moet in deze fase duidelijk worden tot welke gegevens potentieel toegang is, in hoeverre deze toegang noodzakelijk is en hoe zwaar de inbreuk op de privacy is. Dit dient vervolgens tot uitdrukking te komen in het bevel tot de inzet van de hackbevoegdheid. Conform het voorgestelde artikel 125ja, tweede lid, sub e, Sv vermeldt het bevel op welke categorie van gegevens de hack zich richt. Het NJCM is van oordeel dat deze categorie zo concreet mogelijk moet worden omschreven. Daarbij dient de noodzakelijkheid, proportionaliteit en subsidiariteit van iedere separate onderzoekshandeling ten aanzien van deze gegevens worden gemotiveerd.
In de MvT dienen op deze punten de verkennende fase en de motiveringseisen duidelijker benoemd te worden.

2.3 Vrijheid van meningsuiting
Het NJCM wijst op de mogelijke strijdigheid van de hackbevoegdheid met de vrijheid van meningsuiting (artikel 7 Gw en artikel 10 EVRM), zoals verwoord door de Nederlandse Vereniging van Journalisten (NVJ).[3] Het NJCM sluit zich aan bij het voorstel van de NVJ voor het formuleren van een specifieke waarborg voor vrije nieuwsgaring (zie hieromtrent ook paragraaf 4 van deze brief) en bij het voorstel om strengere vereisten aan te leggen voor de bevoegdheid tot ontoegankelijkmaking (nl. een ernstige bezwaren-criterium, beperking tot een kleinere categorie ernstige misdrijven en waarborgen voor het niet langer dan strikt noodzakelijk ontoegankelijk houden).

2.4 Rol van de RC, toestemming en toezicht
De aanwezigheid van rechterlijke toetsing bij de ernstige privacyschending die de inzet van deze opsporingsbevoegdheden oplevert, is met het oog op de geldende jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) aangewezen. Uit paragraaf 2.6 van de Mvt blijkt dat gekozen is voor een dubbele toets: de officier van justitie dient zijn voornemen van het toepassen van de opsporingsbevoegdheden eerst voor te leggen aan de Centrale Toetsingscommissie (CTC), die het College van procureurs-generaal adviseert ten aanzien van de proportionaliteit en subsidiariteit van de inzet. Nadat het College toestemming heeft verleend, legt de officier van justitie zijn vordering aan de rechter-commissaris voor, die eveneens (schriftelijk) toestemming dient te verlenen. Terecht is voor deze rechterlijke toetsing gekozen: de onafhankelijkheid van de rechter-commissaris stelt deze in staat om, in vergelijking tot de rol van de officier van justitie, onpartijdig oordeel te vellen over de vraag of in het belang van het strafrechtelijk onderzoek inbreuken op vrijheid en privacy van verdachten en andere personen kunnen worden gemaakt. Gelet op de mate van inbreuk op de privacy door de genoemde opsporingsbevoegdheden staat het NCJM positief tegenover de keuze van de wetgever voor zowel een interne toets (binnen het Openbaar Ministerie) door de CTC als een rechterlijke toets door de rechter-commissaris.

Het NJCM juicht voorts toe dat er voor stelselmatige observatie met een technisch hulpmiddel nu ook een machtiging van de rechter-commissaris vereist is 'als de desbetreffende

[3] Zie: http://www.nvj.nl/docs/21-6-13_Def_position_paper_cybercrime.pdf.

bevoegdheid wordt toegepast in het kader van onderzoek in een geautomatiseerd werk en het voor de toepassing van de bevoegdheid nodig is dat op afstand heimelijk wordt binnengedrongen in het geautomatiseerde werk' (paragraaf 2.6 van de MvT).

Overigens wijst het NJCM er wel op dat het bij de inzet van deze bevoegdheden gaat om zeer ingewikkelde materie die de rechter-commissaris tot in detail moet bekijken en begrijpen om deze te kunnen beoordelen op noodzakelijkheid en proportionaliteit. De opsporingsbevoegdheden kunnen op veel verschillende manieren worden ingezet, ieder met een eigen consequentie voor de privacy van de betrokkene. De vraag is of een rechter-commissaris (of de CTC) hiervoor in de praktijk voldoende tijd en (ondanks de voorgestelde SSR cursussen) expertise heeft en of op deze wijze wel effectief controle op het handelen van de politie kan worden uitgeoefend. Het NJCM dringt erop aan om na verloop van tijd te evalueren in hoeverre deze kritische toets in de praktijk effectief kan worden uitgevoerd.

2.5 Waarde verkregen informatie als bewijs
Het grote nadeel van digitaal bewijs is dat de betrouwbaarheid problematisch is. Als de overheid een systeem kan hacken, kan een derde dit ook en ligt het gevaar op de loer dat het bewijs gemanipuleerd of vervalst kan worden.
Het bewijsmateriaal is bovendien volledig virtueel en vereist derhalve meerdere bronnen om betrouwbaar te kunnen zijn. Daarnaast heeft bijna elke actie op het bewijs (vaak lezen incluis) invloed op hetgeen digitaal is opgeslagen. Als vervolgens de opsporingsambtenaar ook nog bewijs onbeschikbaar mag maken en mag verwijderen, wordt deze waarde nog minder. Dit kan dus alleen gedaan worden indien voldoende procedures voorhanden zijn om het bewijs veilig te stellen. Digitale bewijsgaring is kortom een onderzoeksgebied op zichzelf, waar al veel richtlijnen voor bestaan. Het NJCM is van mening dat het van groot belang is om deze richtlijnen in acht te blijven houden.

3. Decryptiebevel
In het wetsvoorstel is in artikel 184b Wetboek van Strafrecht een zogenaamd 'decryptiebevel' opgenomen. De minister heeft gekozen voor een zelfstandige strafbaarstelling van het niet voldoen aan een dergelijk bevel, gegeven door de officier van justitie. Het NJCM is van mening dat de ontsleutelplicht buitenproportioneel is en in strijd met het nemo-teneturbeginsel, het recht van een verdachte om zichzelf niet te hoeven belasten.

3.1 (Technische) noodzaak en effectiviteit
Het NJCM betwijfelt of de ontsluitelplicht een effectief middel is, gezien de technische mogelijkheden om zich daartegen te wapenen. Allereerst: cryptografische algoritmes hebben tot doel gegevens er uit te laten zien als volstrekt willekeurige data. Met andere woorden, een versleuteld gegeven is theoretisch niet te onderscheiden van "ruis". In de praktijk worden versleutelde gegevens vaak herkenbaar opgeslagen, zodat er gemakkelijk mee te werken valt. Desalniettemin is het te verwachten dat een capabele verdachte dit ongedaan weet te maken.

Bovendien ondersteunen populaire softwarepakketten vaak functies als een 'schaduw-' of 'paniekwachtwoord'. Dit is een wachtwoord waarmee het lijkt of de data ontsleuteld worden, maar er eigenlijk gegevens achter blijven. Een voorbeeld hiervan is Truecrypt. Ook kent men gedeelde wachtwoorden waarbij meerdere personen tegelijk hun sleutel moeten invoeren.
Ten derde kan men zich wapenen tegen dit bevel door veel gegevensdragers van compleet willekeurige data te voorzien. Het is dan niet meer duidelijk tegen welke gegevensdrager het

verzoek tot ontsleuteling gericht is ofwel het verzoek is onzinnig omdat het tegen willekeurige data gericht is.

Tot slot is het mogelijk een wachtwoord te vernietigen. Cryptografische sleutels dienen momenteel minstens 192 bits te zijn, wat onmogelijk te onthouden is voor een mens. Zodoende komt het erg geloofwaardig over als iemand zegt dat de kopie van de sleutel verloren is geraakt.

3.2 Nemo tenetur

Met het opnemen van een zelfstandige strafbaarstelling heeft de minister voor de meest vergaande optie ten aanzien van het decryptiebevel gekozen. De vraag is hoe dit te rijmen valt met het nemo-teneturbeginsel (artikel 6 EVRM). Het NJCM juicht toe dat de minister uitgebreid onderzoek heeft laten doen naar de verhouding tussen het decryptiebevel en nemo tenetur. Tegelijkertijd baart het het NJCM zorgen dat de minister, ondanks de kritische kanttekeningen die in dit onderzoek naar voren komen ten aanzien van een zelfstandige strafbaarstelling, wel kiest voor deze optie. De minister heeft met deze optie vermoedelijk willen aansluiten bij soortgelijke buitenlandse strafbaarstellingen van het niet meewerken aan een decryptiebevel. Echter, deze strafbaarstellingen zijn nog niet getoetst door het EHRM.

Uit de rechtspraak van het EHRM blijkt dat de vraag of sprake is van een toegestane inbreuk op het nemo-teneturbeginsel afhankelijk is van de aard en mate van dwang, het gewicht van het publiek belang, procedurele waarborgen en de wijze waarop het materiaal wordt gebruikt.[4] Echter, uit die jurisprudentie kan niet worden afgeleid dat aan het nemo-teneturbeginsel bij ernstige strafbare feiten minder gewicht moet worden toegekend; dat beginsel geldt bij feiten als terrorisme onverkort.[5] Juist omdat de ontsleutelplicht veel raakvlakken heeft met het afleggen van een verklaring, en dus de kern van nemo tenetur raakt, dreigt wel degelijk een schending van artikel 6 EVRM.

De voorgestelde zelfstandige strafbaarstelling maakt naar het oordeel van het NJCM een onaanvaardbare inbreuk op het nemo-teneturbeginsel, gezien de mate van dwang zoals die tot uiting komt in de strafbedreiging, en omdat de wettelijke regeling in dit wetsvoorstel met onvoldoende waarborgen is omkleed. Zo is een inbreuk op het nemo-teneturbeginsel door een decryptiebevel in sommige landen slechts aanvaardbaar als voldoende duidelijk is dat de betreffende bestanden daadwerkelijk bestaan en de verdachte de sleutel kent, terwijl in andere gevallen ruimhartige bewijsuitsluitingsregels gelden.

Volgens het NJCM kunnen de betreffende strafbare feiten, hoe ernstig ook, beter worden geadresseerd door toepassing van een minder vergaande wijze van het gebruik van een decryptiebevel. Een decryptiebevel met verschoningsrecht[6] past beter in het Nederlandse rechtssysteem en biedt een passender waarborg ten aanzien van het nemo-teneturbeginsel.

---

[4] B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel,* Tilburg: TILT 2012, p. 103.

[5] EHRM 21 december 2000, *EHRC* 2001, 18 (Quinn/Ierland); EHRM 21 december 2010, appl. no. 34720/97 (Heaney & McGuinness/Ierland). Zie D. van Toor, 'Het decryptiebevel en het nemo-teneturbeginsel', *NJB* 2013, p. 477-479.

[6] Koops 2012, p. 90-91.

3.3 Recht op bescherming persoonlijke levenssfeer
In de MvT wordt geconcludeerd dat gebruik van het decryptiebevel kan leiden tot een inbreuk op de eerbiediging van de persoonlijke levenssfeer. Volgens de opsteller voldoet het decryptiebevel aan de vereisten van artikel 10 van de Grondwet en artikel 8 van het EVRM en is daarmee een inbreuk op de eerbiediging van de persoonlijke levenssfeer gerechtvaardigd.
Bij de bespreking van deze vereisten wordt summier aandacht besteed aan beginselen van proportionaliteit en subsidiariteit en wordt voorbijgegaan aan het feit dat de computer tegenwoordig meer privacygevoelige informatie bevat dan voorheen. Enkele jaren geleden werden zo nu en dan bestanden door de computergebruiker op diens computer opgeslagen. Thans bevat de computer méér privacygevoelige informatie: elektronische agenda's, elektronische post, chatgesprekken, et cetera. Het gebruik van het decryptiebevel brengt met zich mee dat óók dit onder de loep wordt genomen en dat als gevolg hiervan meer privacygevoelige informatie wordt gevonden dan bij een huiszoeking.

Bovendien valt met het instellen van een hackbevoegdheid voor de opsporingsdiensten de noodzaak van het hebben van een ontsleutelplicht weg. Op het moment dat de opsporingsambtenaar het recht heeft om een geautomatiseerd systeem binnen te dringen kan hij a) de sleutels uit het geheugen extraheren als de versleuteling recent heeft plaatsgevonden of b) het systeem net zo lang monitoren totdat de verdachte zijn sleutel invoert en deze afluisteren. Dit geldt overigens ook voor de dataretentie. Met het invoeren van deze wet zou de noodzaak voor de dataretentiewet bovendien deels wegvallen, omdat de opsporingsambtenaar voldoende andere bronnen voorhanden heeft.

Het NJCM is van oordeel dat de proportionaliteit en subsidiariteit van de bevoegdheid nog onvoldoende zijn aangetoond in het licht van de grote hoeveelheid privacygevoelige informatie die gegevensdragers in het huidige elektronische tijdperk bevatten.

4. 'Heling' en 'verduistering' van gegevens
Het wetsvoorstel beoogt 'heling' en 'verduistering' van gegevens strafbaar te stellen in de voorgestelde artikelen 138c Sr en 139f Sr. Het NJCM juicht toe dat hiermee beter wordt aangesloten op de snel veranderende praktijk van cybercrime, maar is tegelijkertijd kritisch over het mogelijke 'chilling effect' op de vrije nieuwsgaring (artikel 7 Gw en artikwl 10 EVRM) die de voorgestelde bepalingen creëren.

Het wetsvoorstel beoogt onder andere klokkenluiders en journalisten uit te zonderen van strafbaarheid. Dit komt in artikel 138c Sr tot uiting in het bestanddeel wederrechtelijk, terwijl aan artikel 139f Sr een apart lid is toegevoegd dat expliciet bepaalt dat van strafbaarheid geen sprake is als de betrokkene te goeder trouw heeft kunnen aannemen dat het algemeen belang bekendmaking van de gegevens vereiste. Hoewel het aanbrengen van een zelfstandige waarborg in het tweede lid van artikel 139f toe te juichen valt, betwijfelt het NJCM of de huidige algemene formulering wel de beoogde waarborg voor de vrije nieuwsgaring kan bieden. Het NJCM zou graag nader in de wet geëxpliciteerd willen zien dat activiteiten van journalisten en klokkenluiders – en degenen die hen faciliteren – niet onder deze strafbaarstelling vallen, tenzij een dergelijke beperking strikt noodzakelijk en proportioneel is (zie artikel 10, tweede lid, EVRM).

Een dergelijke exceptie dient naar het oordeel van het NJCM ook te worden aangebracht bij artikel 138c, gezien het mogelijke 'chilling effect' op de vrije nieuwsgaring die reeds uitgaat van een strafbaarstelling van in het stadium van het overnemen van gegevens.

Bovendien is het voorgestelde artikel 138c nu dusdanig ruim geformuleerd dat de vrijheidssfeer van burgers in de digitale wereld daar sterk door beperkt kan worden. De voorgestelde wetsbepaling geeft niet nader aan wat precies strafbaar is aan het overnemen van niet-openbare gegevens, zodat alles aankomt op de vraag wat dan wederrechtelijk is. Dit creëert naar het oordeel van het NJCM teveel rechtsonzekerheid. De MvT geeft aan dat een beperking van het artikel tot 'gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat openbaarmaking of verspreiding de persoonlijke levenssfeer kan schenden' niet wenselijk is, omdat ook 'gegevens [kunnen] worden overgenomen uit overwegingen van geldelijk gewin zonder dat schending van de persoonlijke levenssfeer daarbij aan de orde is.' In dit opzicht kan volgens het NJCM het beste gekozen worden voor een beperking van de reikwijdte van het artikel tot gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat openbaarmaking of verspreiding de persoonlijke levenssfeer kan schenden en gegevens die worden overgenomen uit overwegingen van geldelijk gewin. Op deze manier wordt bereikt dat de strafbaarstelling zo min mogelijk inbreuk maakt op de vrijheidssfeer van burgers en het strafrecht laatste redmiddel blijft.

5. Soevereiniteitskwestie en cybercrimeverdrag

De minister kiest ervoor om vooruitlopend op internationale afspraken de opsporingsbevoegdheden bij de bestrijding van cybercrime in Nederland uit te breiden. Door het internationale karakter van cybercrime is niet altijd duidelijk waar een computer zich bevindt en bij de opsporing is snelheid vaak geboden. De minister wil dat in die gevallen de bevoegdheden zonder voorafgaand rechtshulpverzoek kunnen worden toegepast, ongeacht waar de computer en de gegevens zich op dat moment bevinden.
Het NJCM merkt op dat handhavend optreden buiten het eigen territorium van de Staat – extraterritoriale handhaving – in beginsel onrechtmatig is onder het internationaal recht. Ook voor het verkrijgen van informatie voor een juridische procedure is in principe instemming van de betrokken vreemde Staat nodig. Het verdient daarom de voorkeur om nadere internationale afspraken over dit onderwerp te maken. Hier komt nog bij dat wanneer andere landen het voorbeeld van Nederland in dezen zullen volgen ook de soevereiniteit van Nederland geschonden kan worden. Tot slot kan men betwijfelen of het mogelijk is om cybercrime daadwerkelijk effectief te bestrijden zonder internationale samenwerking.

Het NJCM ziet met verwachting uit naar het vervolg van het wetgevingstraject en is graag bereid om daar verder over mee te denken.

Hoogachtend,

Marloes van Noorloos
Voorzitter NJCM