Eerste Kamer der Staten-Generaal
T.a.v. de vaste commissie voor Veiligheid en Justitie
postbus@eerstekamer.nl

Leiden, 16 mei 2017
Betreft: wetsvoorstel Computercriminaliteit III

Geachte Kamerleden,

Op 2 december 2016 heeft het Nederlands Juristen Comité voor de Mensenrechten (NJCM) in een brief aan de vaste commissie voor Veiligheid en Justitie van de Tweede Kamer zijn zorgen geuit over het wetsvoorstel Computercriminaliteit III.[1] Dit naar aanleiding van een eerdere reactie tijdens de internetconsultatie (op 28 juni 2013)[2] en omdat er, ondanks aanpassingen in het wetsvoorstel en de memorie van toelichting (MvT) en na beantwoording van vragen in de nota van 8 november 2016, nog punten waren die het NJCM zorgen baarden. Desondanks is dit wetsvoorstel op 20 december 2016 door de Tweede Kamer aangenomen. Nu het wetsvoorstel ter goedkeuring ligt van de Eerste Kamer, en onze zorgen nog niet zijn weggenomen, vragen wij uw aandacht voor onderstaande punten.

1 Privacyvragen en -waarborgen hacken

1.1 Reikwijdte

Het NJCM heeft aangegeven dat het wetsvoorstel, blijkens de titel, gericht is op de verbetering en versterking van de opsporing en vervolging van computercriminaliteit. Toch heeft de staatssecretaris 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. Betekent dit dat de hackbevoegdheid tot een algemeen opsporingsmiddel is verworden? In de MvT (paragraaf 8.1) staat dat de keuze voor de categorie van misdrijven, waarbij de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk kan worden toegepast, is ingegeven door het in ernstige mate hinderen van de opsporing van dergelijke misdrijven doordat het niet mogelijk is binnen te dringen in een geautomatiseerd werk.[3] Toch is de bevoegdheid niet beperkt tot bepaalde (soorten) delicten, maar slechts tot delicten van een bepaalde ernst.

[1] Brief aan de vaste commissie voor Veiligheid en Justitie van de Tweede Kamer, 2 december 2016, zie : https://njcm.nl/wp-content/uploads/2016/12/Reactie-NJCM-nav-consultatie-Computercriminaliteit-III_DEF.pdf
[2] NJCM-inbreng 'Consultatie conceptwetsvoorstel versterking bestrijding computercriminaliteit', 28 juni 2013, zie: https://njcm.nl/wp-content/uploads/2017/01/NJCMinbreng_internetconsultatie_computercriminaliteitIII.pdf
[3] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 79-80 (MvT).

Ook in paragraaf 2.2 van de MvT staat dat het toepassingsbereik van onderzoek in een geautomatiseerd werk zich niet beperkt tot specifieke gevallen van computercriminaliteit, zoals computervredebreuk:

> 'De bevoegdheid kan ook ten aanzien van andere misdrijven worden toegepast, waarvoor op grond van artikel 67 eerste lid Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. Dit omdat ook bij het voorbereiden en plegen van meer traditionele misdrijven, als moord, handel in drugs en mensenhandel, het gebruik van moderne ICT-voorzieningen een steeds belangrijker component is geworden, bijvoorbeeld als het gaat om communicatie tussen criminelen.'[4]

Het NJCM juicht het niettemin toe dat de bevoegdheid nader wordt ingekaderd. Dit was al het geval door beperking tot misdrijven waarvoor voorlopige hechtenis mogelijk is, en heeft nu ook vorm gekregen door beperking van bepaalde onderzoekshandelingen tot misdrijven waarop een gevangenisstraf van acht jaar of meer is gesteld of die bij algemene maatregel van bestuur zijn aangewezen. Echter, van de limitatieve opsomming zoals voorgesteld door het NJCM, is geen sprake. Het aantal misdrijven waarbij het onderzoek in een geautomatiseerd werk kan worden toegepast blijft groot. Hierdoor kunnen de middelen veel te breed worden ingezet en kunnen de vrijheden van burgers in het geding komen. Inmiddels hebben ook Kamerleden van verschillende fracties hun zorgen geuit over het grote aantal misdrijven waarbij de hackbevoegdheid toegepast kan worden.[5] Als de bevoegdheid een laatste redmiddel is, zoals in de MvT is benadrukt in reactie op het advies van Bits of Freedom,[6] dan zou deze niet zo ruim mogen zijn.

1.2 Privacyvragen hacken

Het NJCM heeft zijn zorgen geuit met betrekking tot de mogelijk verregaande inbreuk op de privacy die inzet van een hackbevoegdheid zou kunnen betekenen, niet alleen voor verdachten, maar ook voor huisgenoten of andere derden. Hieraan wordt grotendeels tegemoetgekomen door de voorbereidingsprocedure ('verkenningsfase'), zoals omschreven in paragraaf 2.5 van de MvT,[7] en de eisen die worden gesteld aan het bevel tot inzet van de bevoegdheid waarin de te verrichten handelingen, het te onderzoeken deel van het geautomatiseerde werk en de periode waarin mag worden onderzocht, moeten worden vermeld.[8] Het voorstel van het NJCM om een motivering te vereisen per te verrichten onderzoekshandeling is tot onze spijt niet overgenomen. Hiermee is een kans gemist om de privacy beter te waarborgen én om de controleerbaarheid van de opsporing te vergroten.

Daarnaast valt op dat de eisen die aan het bevel van de officier van justitie worden gesteld minder uitgebreid zijn wanneer er sprake is van aanwijzingen van een terroristisch misdrijf. In het voorgestelde artikel 126zpa, vallen t.o.v. de artikelen 126nba en 126uba sub g en h weg in het tweede lid. Hiermee vervalt onder andere de beperking van de bevoegdheid tot inzet op een bepaald tijdstip of binnen een bepaalde periode. Vanzelfsprekend is de opsporing van terroristische misdrijven van groot belang, maar zonder verdere onderbouwing is niet duidelijk wat

---

[4] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 15 (MvT).

[5] *Kamerstukken II* 2015/16, 34372, nr. 5, p. 12, 14-15 (Verslag).

[6] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 79 (MvT).

[7] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 32-34 (MvT) en *Kamerstukken II* 2016/17, 34372, nr. 6, p. 14 (Nota).

[8] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 30 (MvT).

de noodzaak is achter de genoemde beperking van waarborgen. Bij terroristische misdrijven is al een veel minder sterke verdenking vereist voor inzet van de bevoegdheid. Wanneer het bevel ook nog voor onbeperkte tijd wordt gegeven, lijkt de inbreuk op de privacy van (mogelijke) verdachten niet in verhouding te staan tot de noodzaak ervan. De keuze voor deze verdere verruiming van de bevoegdheid zou op zijn minst nader moeten worden onderbouwd.

1.2.1 Bewaartermijn

In het voorgestelde artikel 126cc, zesde lid staat dat gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk, worden vernietigd zodra blijkt dat zij van geen betekenis zijn voor het onderzoek. Het NJCM vindt dit te vrijblijvend. Het wetsvoorstel zou moeten voorzien in een uiterste termijn waarna gegevens in elk geval moeten worden vernietigd. In het huidige voorstel is dit niet het geval, waardoor de vrees ontstaat dat veel gegevens lange tijd zullen worden bewaard in de veronderstelling dat zij ooit nog van pas zullen komen. Hierdoor ontstaat het risico van inbreuken op de privacy van vele gewezen (of niet geworden) verdachten. Dit speelt vooral in zaken waarin wel onderzoek wordt gedaan, maar uiteindelijk geen vervolging tot stand komt. Aansluiting bij de bewaartermijnen van de Wet politiegegevens, zoals aangegeven in de nota,[9] lijkt niet afdoende gelet op de zeer privacygevoelige informatie die met de voorgestelde bevoegdheden kan worden verkregen.

1.3 Vrijheid van meningsuiting

In het kader van de vrijheid van meningsuiting is tijdens de consultatie vooral gewezen op de vrijheid van journalisten. Dit komt in paragraaf 4 verder aan de orde.

1.4 Rol van de RC, toestemming en toezicht

In de consultatieronde is al waardering uitgesproken voor de rechterlijke toets door de rechter-commissaris, naast de interne toets door de Centrale Toetsingscommissie (CTC) van het Openbaar Ministerie. Deze juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid, naast bijvoorbeeld het vereiste van het dringende onderzoeksbelang, moeten een zorgvuldige afweging waarborgen voordat de voorgestelde bevoegdheid wordt ingezet. Het NJCM is echter van mening dat de CTC onvoldoende onafhankelijk is, aangezien het is samengesteld uit leden van het Openbaar Ministerie en de politie. Het NJCM pleit voor structureel onafhankelijk toezicht door een toezichtcommissie zoals de CTIVD, die de inlichtingen- en veiligheidsdiensten controleert. Het NJCM wijst er bovendien op dat uit de jurisprudentie omtrent artikel 8 EVRM duidelijk blijkt dat het onafhankelijk toezicht niet alleen gaat over het verlenen van de toestemming vooraf door een toezichthoudend orgaan, maar ook over het tijdens de procedure kunnen beëindigen daarvan.[10] Wat het NJCM mist in het voorstel is onafhankelijk toezicht tijdens en, in de gevallen die niet tot vervolging leiden, na afloop van de procedure. Het NJCM acht het een gemiste kans dat hier niet is gekozen voor uitbreiding van de bevoegdheid van de rechter-commissaris.

---

[11] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 41-42 (Nota).

[10] Zie bijv. het Gerechtshof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881, r.o. 2.9: '….dat onafhankelijk toezicht in de door het EHRM bedoelde zin niet denkbaar is indien het toezichthoudende orgaan niet op zijn minst de bevoegdheid heeft om het direct of indirect tappen van advocaten te voorkomen of te beëindigen.'

De uitwerking die in de MvT is gegeven aan het voorzien in voldoende kennis en expertise bij het OM en de rechterlijke macht onderschrijft het NJCM graag.

1.5 Waarde verkregen informatie als bewijs

In de MvT wordt ten opzichte van de conceptversie kort ingegaan op de betrouwbaarheid van het bewijs. Vooral wordt beargumenteerd dat de politie er geen belang bij heeft om zwakheden en kwetsbaarheden in systemen uit te buiten en te laten bestaan. Dit bevreemdt enigszins, aangezien het bestaan van de mogelijkheid om de computer van een verdachte te hacken nu juist afhankelijk is van dergelijke zwak- en kwetsbaarheden. Hoewel in de nota naar aanleiding van het verslag wordt aangegeven dat gebruik van een kwetsbaarheid niet de meest aangewezen methode is voor het binnendringen in een geautomatiseerd werk, blijft het wel degelijk een bruikbare methode.[11] Het is er tevens een waarvan het kabinet in de brief van 8 november 2016 heeft aangegeven het gebruik niet uit te sluiten.

De door het NJCM tijdens de consultatie aangevoerde bezwaren blijven gelden, namelijk dat volledig virtueel bewijsmateriaal meerdere bronnen vereist om voldoende betrouwbaar te zijn en makkelijk kan worden gemanipuleerd of vervalst. Zo heeft vrijwel elke handeling (ook enkel lezen) al effect op de staat van het bewijs. Als opsporingsambtenaren dan ook nog gegevens ontoegankelijk mogen maken of mogen verwijderen, rijst de vraag of de betrouwbaarheid en reproduceerbaarheid voldoende zijn in het licht van de bewijsrechtelijke eisen die aan een eerlijk proces gesteld worden. In de MvT wordt hier onvoldoende op in gegaan.

2 ‘Heling’ en ‘verduistering’ van gegevens

Het NJCM heeft zijn zorgen geuit over de strafbaarstellingen van de voorgestelde artikelen 138c en 139g Sr, in het bijzonder vanwege de ‘chilling effect’ dat deze bepalingen zouden kunnen hebben op vrije nieuwsvergaring binnen de onderzoeksjournalistiek. Het is goed te zien dat in de huidige formulering van het tweede lid van artikel 139g naast bekendmaken ook het verwerven, voorhanden hebben, ter beschikkingstellen en gebruiken onder voorwaarden zijn uitgezonderd van strafbaarheid. De expliciete vermelding van journalisten en klokkenluiders in de MvT (p. 66) en later in de nota naar aanleiding van het verslag (p. 111-113) geven bovendien blijk van erkenning voor de bescherming die deze groepen nodig hebben.

Ten aanzien van het voorgestelde artikel 138c echter, betreurt het NJCM dat deze strafbaarstelling niet verder is ingeperkt en dat het eventueel wegnemen van het strafbare karakter van deze handelingen nog steeds enkel afhankelijk is van de vraag of niet-openbare gegevens wederrechtelijk zijn overgenomen. Hoewel een strafbaarstelling afhankelijk van de motivatie die een verdachte voor zijn handelen had (zoals geldelijk gewin) bij nader inzien niet wenselijk voorkomt, acht het NJCM enige verdere beperking van de reikwijdte van artikel 138c meer dan gewenst.

[11] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 38 (Nota).

3 Soevereiniteitskwestie en cybercrimeverdrag

Het is goed om te zien dat de huidige MvT, meer dan de versie die in consultatie beschikbaar was, rekenschap geeft van de moeilijkheden die zich omtrent rechtsmacht en soevereiniteit kunnen voordoen bij de inzet van de voorgestelde opsporingsbevoegdheden. Ook is het positief dat vermelding hiervan een voorgeschreven onderdeel is van het bevel van de officier van justitie. Het NJCM geeft evenwel de voorkeur aan inzet via formele rechtshulpverzoeken en aan het vastleggen van procedures en waarborgen in internationale afspraken.

Hoewel het NJCM blij is met een aantal aanpassingen op het wetsvoorstel Computercriminaliteit III, blijven wij zorgen houden over waarborgen van de privacy ten opzichte van de opsporing en de effectiviteit van de voorgestelde bevoegdheden. Wat het NJCM betreft zijn de belangrijkste knelpunten: de reikwijdte van het voorstel en daarmee de (mogelijke) inbreuk op de privacy, het ontbreken van voldoende onafhankelijk toezicht, het mogelijk langdurig bewaren van gegevens en de beperkte controleerbaarheid van bewijs in het strafproces. Wij hopen dat u onze zorgen bij de bespreking in de Eerste Kamer wilt betrekken.

Hoogachtend,

i/o

Ton van den Brandt
Voorzitter NJCM

Sterrenwachtlaan 11 – 2311 GW Leiden – 071-527 77 48 – NJCM.nl – KvK 40445896