Tweede Kamer der Staten-Generaal
Leden van de Vaste commissie voor Veiligheid en Justitie

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

t (070) 361 97 23
f (070) 361 97 15
www.rechtspraak.nl

datum 10 februari 2016
onderwerp Rondetafelgesprek Wetsvoorstel computercriminaliteit III 11 02 2016

De Raad voor de rechtspraak (de "**Raad**") dankt de Vaste commissie voor Veiligheid en Justitie voor de uitnodiging voor dit rondetafelgesprek. De Raad heeft ondergetekende gevraagd om vanuit mijn expertise als senior raadsheer in het Gerechtshof Den Haag, voorzitter van de zogeheten cyberkamer van dit hof en coördinator van het landelijke Kenniscentrum Cybercrime vanuit de Rechtspraak aan dit gesprek deel te nemen. Dit wil overigens – voor de goede orde – niet zeggen dat mijn bijdrage in zijn geheel per se overeenkomt met reeds door de Raad in het kader van zijn wettelijke adviseringsrol ingenomen formele standpunten.

Het wetsvoorstel computercriminaliteit-III heeft een lange voorgeschiedenis.[1] Gezien het feit dat het hier deels om nieuwe opsporingsbevoegdheden gaat die een vergaande inbreuk op grondrechten van burgers (verdachten of derden) opleveren kan daar begrip voor worden opgebracht. Hier dient immers grote zorgvuldigheid te worden betracht. De Raad constateert met genoegen dat in het voortraject niet alleen vele belanghebbenden zijn geraadpleegd, maar dat met die inbreng ook daadwerkelijk iets is gedaan. De Raad hecht daarbij in het bijzonder aan de aanpassingen ten opzichte van het concept-wetsvoorstel met betrekking tot het encryptiebevel en de verhoging van de drempel voor het mogen binnendringen in een geautomatiseerd werk en voor het ontoegankelijk maken van gegevens. Ook positief beoordeelt de Raad de vele juridische technische aanpassingen van het concept-wetsvoorstel, waardoor het thans voorliggende wetsvoorstel aan duidelijkheid en uitvoerbaarheid heeft gewonnen.

Hoewel de Raad op meerdere onderdelen van het wetsvoorstel nog de nodige juridische probleem- en vraagpunten ziet, zal ik mijn inbreng beperken tot twee punten, die thans als het meest zwaarwegend kunnen worden aangemerkt. Dat betreft allereerst het punt van de toetsing achteraf van de inzet van het opsporingsmiddel "binnendringen in een geautomatiseerd werk" (art. 126nba Sv). Het tweede punt betreft de problematiek van het extra-territoriaal inzetten van dit opsporingsmiddel.

1. **Toetsing achteraf van de inzet van het opsporingsmiddel "binnendringen in een geautomatiseerd werk" (art. 126nba Sv).**

In de systematiek van het wetsvoorstel zal, indien inzet van dit opsporingsmiddel wordt overwogen, daarvoor eerst door een officier van justitie binnen de hiërarchie van het Openbaar Ministerie bijzondere toestemming moeten worden verkregen. Indien deze toestemming is verkregen, zal de officier van justitie, alvorens een

[1] Zie ook de adviezen van de Raad van 30 september 2010, 4 juli 2013 en 10 oktober 2014, alle gepubliceerd op www.rechtspraak.nl.

bevel te kunnen geven dit middel ook in te zetten, daarvoor tevens de machtiging behoeven van de rechter-commissaris in strafzaken. Deze zal daartoe het verzoek van de officier van justitie toetsen op rechtmatigheid, proportionaliteit en subsidiariteit. Indien de rechter-commissaris van mening is dat aan deze eisen is voldaan, zal de machtiging worden verleend.

Graag vraag ik er aandacht voor dat dit slechts een toetsing *vooraf* op de inzet van het opsporingsmiddel is, waarbij de rechter-commissaris bij zijn beoordeling bovendien volledig afhankelijk is van de juistheid en de omvang van de informatie die hem vanuit de politie en de officier van justitie wordt verstrekt. Indien geen verlenging wordt gevraagd, zal de rechter-commissaris ook geen zicht (kunnen) hebben op de wijze waarop met de eerder door hem verstrekte machtiging is omgegaan. De oorspronkelijke gedachte achter het Wetboek van Strafvordering was en is daarbij dat de inzet van deze opsporingsmiddelen vervolgens ook achteraf kan worden (of in ieder geval zou kunnen worden) getoetst door de zittingsrechter. Het volledige dossier behoort dan beschikbaar te zijn, en ingevolge het systeem van checks en balances kan de verdediging dan ook andere informatie aandragen dan die welke reeds in het dossier aanwezig is.

Het is echter juist een kenmerk van met name zaken welke zich in cyberspace afspelen, dat het veelal wel mogelijk blijkt de datastroom te volgen, maar dat het buitengewoon moeilijk blijkt daaraan ook individuele verdachten te koppelen. Dat kan zijn omdat zij zich achter anonimiteit verschuilen, maar ook omdat zij zich feitelijk bevinden in landen die geen medewerking verlenen aan het onderzoek of die verdachten niet uitleveren. In deze gevallen, maar ook in andere gevallen, waarin uiteindelijk niet tot een vervolging (in Nederland) wordt besloten, zal derhalve geen toetsing *achteraf* van de inzet van de digitale binnendringingsbevoegdheid meer plaatsvinden. Gezien de impact die de inzet van dit middel kan hebben en de maatschappelijke risico's die kunnen ontstaan indien opsporingsdiensten zulke vergaande middelen kunnen inzetten zonder dat deze inzet achteraf nog wordt gecontroleerd/getoetst, wordt aan het - waarschijnlijk in een aanzienlijk aantal gevallen - ontbreken van de rechterlijke toetsing achteraf in (de Memorie van Toelichting bij) het wetsvoorstel ten onrechte geen aandacht besteed.

Ik kan me voorstellen dat nader wordt onderzocht in hoeverre in deze lacune zou kunnen worden voorzien door het instellen van een Commissie van Toezicht, vergelijkbaar met de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten. Een dergelijke commissie zou dan achteraf toezicht uit kunnen oefenen op de rechtmatigheid van de uitvoering van de bevoegdheid als genoemd in artikel 126nba Sv en daarvan (grotendeels) openbaar verslag kunnen doen. Voorwaarde zal dan wel moeten zijn dat zo'n commissie inzicht krijgt in alle gewenste gegevens.

2. De extra-territorialiteitsproblematiek

In de voorbereiding van dit wetsvoorstel, alsook in de Memorie van Toelichting is aandacht besteed aan de problematiek van de toepassing van de binnendringingsbevoegdheid in het geval de lokatie van het geautomatiseerde werk niet kan worden gelokaliseerd of dat geautomatiseerde werk zich in het buitenland bevindt. De Raad heeft over een eerdere versie van het wetsvoorstel al opgemerkt dat desondanks het wetsvoorstel geen duidelijke normen stelt ten aanzien van de gevallen waarin dan wel, dan wel niet, van deze bevoegdheid gebruikt zou mogen worden gemaakt, en dat is nog steeds niet het geval. De enkele verwijzing naar een inhoudelijk nog onbekende amvb, zoals thans voorzien in artikel 126nba, lid 8 Sv, of beschouwingen daaromtrent in de Memorie van Toelichting lijken in dit opzicht zowel vanuit rechtstatelijk als vanuit

internationaalrechtelijk perspectief voor de rechtspraktijk onvoldoende aanknopingspunten voor beoordeling te bieden. Ik acht het ook minder gewenst dat deze normering zal worden vormgegeven in een Aanwijzing danwel een amvb, zoals thans in de Memorie van Toelichting genoemd, reeds omdat niet goed valt in te zien hoe deze ook leidend zou kunnen zijn voor de onafhankelijke toetsing door de rechter(-commissaris).

Aandacht verdient het feit dat, zoals ook in het rapport van prof. Koops[2] is omschreven, thans nog geen internationaalrechtelijke basis lijkt te bestaan voor de inzet van deze bevoegdheid op buiten Nederland gelegen geautomatiseerde werken. Men kan zich hier de vraag stellen of de Memorie van Toelichting op dit punt niet meer een zeker justitieel wenselijkheidsdenken weergeeft dan de juridische en politieke realiteit. De Raad wees er in dit verband al op dat, anders dan de Memorie van Toelichting suggereert, bijvoorbeeld ook het Cybercrimeverdrag niet toestaat dat er grensoverschrijdend streaming data wordt “afgetapt”, welke mogelijkheid echter in het wetsvoorstel in art. 126nba, lid 1 onder d. Sv nadrukkelijk wel als een van de functionaliteiten van de binnendringingsbevoegdheid is opgenomen.

Ik wil er in dit verband ook aandacht voor vragen dat het zonder voldoende internationaal- rechtelijke basis inzetten van de binnendringingsbevoegdheid op buitenlandse geautomatiseerde werken ook risico’s oplevert voor het daarbij betrokken justitiële personeel. Zij zullen zich dan namelijk naar het recht van zeer vele landen schuldig maken aan het misdrijf van computervredebreuk, met alle gevolgen van dien. Die strafrechtelijke aansprakelijkheid kan zich ook uitstrekken tot de officier van justitie en de rechter-commissaris. Daarboven dringt zich de integriteitsvraag op of men van justitiële ambtenaren kan vragen gebruik te maken van een opsporingsmiddel dat – naar brede juridische opvatting – in zo’n geval niet rechtmatig mag worden ingezet.

Tot op zekere hoogte lijkt vanuit het internationale recht wel verdedigbaar dat in uitzonderlijke gevallen, waarin grote belangen op het spel staan, aan een staat een zeker zelfverdedigingsrecht toekomt, met name om aan een bedreiging feitelijk een einde te maken. In dit verband verdient het, zoals ook reeds door de NOvA naar voren gebracht, naar het oordeel van de Raad serieuze overweging of niet – naar Duits voorbeeld – in de wet moet worden vastgelegd dat toepassing van voormelde bevoegdheid, of van bepaalde onderdelen van die bevoegdheid, op geautomatiseerde systemen waarvan op enig moment blijkt dat zij zich in het buitenland bevinden slechts in bijzondere gevallen zal mogen plaatsvinden, namelijk die waarin sprake is van:
1) lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen of
2) van gemeen gevaar voor goederen, dat een bedreiging oplevert voor het voortbestaan van de staat of de mensheid.

Met vriendelijke groet,

Mr. Chr. A. Baardman
Senior raadsheer Gerechtshof Den Haag / Coördinator Kenniscentrum Cybercrime

[2] Zie B.J. Koops & M. Goodwin (2014), Cyberspace, the cloud, and cross-border criminal investigation.