0 BD

de Rechtspraak

Raad voor de rechtspraak

04-04-2014 14:52

De Minister van Veiligheid en Justitie
mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

Afdeling Strategie

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

T (088) 36 10000
F (088) 36 10022
www.rechtspraak.nl

datum	3 april 2014
contactpersoon	
e-mail	
telefoonnummer	
ons kenmerk	
uw kenmerk	
onderwerp	Advies Wetsvoorstel implementatie richtlijn aanvallen op informatiesystemen
bijlage(n)	1

Geachte heer Opstelten,

Bij brief van 3 februari 2014, ontvangen op 7 februari 2014, met bovengenoemd kenmerk verzocht u de Raad voor de rechtspraak (de "**Raad**") u te adviseren over het Wetsvoorstel Implementatie richtlijn aanvallen op informatiesystemen (het "**Wetsvoorstel**").

Wetsvoorstel
Het Wetsvoorstel strekt blijkens de Memorie van Toelichting ("**MvT**") tot implementatie van de richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PbEU L218/8) (de "**Richtlijn**"). Volgens de MvT voldoet Nederland voor een groot deel al aan hetgeen waartoe de Richtlijn verplicht. De implementatie van de Richtlijn leidt tot enkele aanscherpingen van strafbaarstellingen van computercriminaliteit in het Wetboek van Strafrecht, te weten een aantal verhogingen van strafmaxima en de toevoeging van een aantal strafverzwarende omstandigheden aan de computerdelicten.

Gehoord de gerechten, adviseert de Raad als volgt.[1]

[1] De Raad voor de rechtspraak heeft op grond van artikel 95 van de Wet op de rechterlijke organisatie een wettelijke adviestaak met betrekking tot nieuwe wets- en beleidsvoorstellen die gevolgen hebben voor de rechtspraak. De adviezen worden vastgesteld na overleg met de gerechten. De Raad voor de rechtspraak is een adviescollege in de zin van artikel 79 en 80 van de Grondwet. Bij het opstellen van zijn adviezen beoordeelt de Raad de voorgenomen wet- en regelgeving in het bijzonder op de gevolgen voor de organisatie en de werklast van de gerechten en op de (praktische) toepasbaarheid en uitvoerbaarheid. Rechters zijn bij de behandeling van individuele zaken niet gebonden aan de inhoud van de wetgevingsadviezen van de Raad voor de rechtspraak.

de Rechtspraak

Raad voor de rechtspraak

Advies
De Raad heeft kennisgenomen van het Wetsvoorstel. Het Wetsvoorstel geeft aanleiding tot het maken van enkele opmerkingen van juridisch-technische aard. Deze zijn opgenomen in een bijlage bij dit advies. Het Wetsvoorstel geeft verder geen aanleiding tot het maken van inhoudelijke opmerkingen.

Werklastgevolgen
Het Wetsvoorstel zal naar verwachting voor de Rechtspraak geen noemenswaardige werklastgevolgen met zich brengen.

Tot slot
Indien na het uitbrengen van dit advies het Wetsvoorstel op belangrijke onderdelen wordt gewijzigd of indien uit nadere uitvoeringsregelgeving belangrijke werklastgevolgen voortvloeien, wordt de Raad graag in de gelegenheid gesteld daarover aanvullend te adviseren. Met het oog op de informatievoorziening aan en de voorbereiding van de gerechten op de invoering van de onderhavige regeling verzoekt de Raad u hem te informeren over de indiening van het wetsvoorstel bij de Tweede respectievelijk de Eerste Kamer en de plaatsing van de definitieve wettekst in het Staatsblad.

Hoogachtend,

Lid Raad voor de rechtspraak

Bijlage: opmerkingen van juridisch-technische aard

- **Artikel 3 van de Richtlijn**

Artikel 3 van de Richtlijn verplicht de lidstaten tot het treffen van de nodige maatregelen om de opzettelijke en onrechtmatige toegang tot een informatiesysteem of een deel daarvan strafbaar te stellen wanneer het strafbaar feit is gepleegd door een beveiligingsmaatregel te doorbreken, althans voor gevallen die niet onbeduidend zijn. Volgens de MvT komt dit artikel overeen met artikel 2 van het Cybercrimeverdrag.

Artikel 2 van het Cybercrimeverdrag luidt echter als volgt: *"Iedere Partij neemt de wetgevende en andere maatregelen die nodig zijn om in haar nationale wetgeving als strafbaar feit aan te merken het opzettelijk en wederrechtelijk verwerven van toegang tot een computersysteem of een onderdeel daarvan. Een Partij kan als voorwaarde voor strafbaarheid stellen dat het feit wordt begaan door het doorbreken van veiligheidsmaatregelen, of met het oogmerk computergegevens te verkrijgen of met het oogmerk van andere oneerlijke bedoelingen, dan wel met betrekking tot een computersysteem dat met een ander computersysteem is verbonden."*

Aandacht verdient hierbij het al dan niet als vereiste stellen dat er sprake moet zijn van een doorbreking van een beveiligingsmaatregel. In de MvT wordt terecht verwezen naar de strafbaarstelling in artikel 138ab, eerste lid, Sr. Artikel 138ab Sr spreekt over vier gevallen waarin in ieder geval sprake is van binnendringen in een geautomatiseerd werk. Blijkens de tekst van dit artikel en de wetsgeschiedenis is dit een niet-limitatieve opsomming van alternatieven. Eén van die gevallen betreft het doorbreken van een beveiliging. Ingevolge het Cybercrimeverdrag is er door de wetgever voor gekozen om het doorbreken van een beveiliging niet als vereiste te stellen om te kunnen spreken van het binnendringen van een geautomatiseerd werk. De Richtlijn lijkt deze voorwaarde wel te stellen.

- **Artikelen 4 en 5 van de Richtlijn**

Artikelen 4 en 5 van de Richtlijn verplichten de lidstaten de nodige maatregelen te treffen om onrechtmatige systeemverstoringen respectievelijk onrechtmatige gegevensverstoring strafbaar te stellen. Volgens de MvT zijn de in dit artikel genoemde gedragingen thans reeds strafbaar op grond van artikel 138b, 161sexies en 350a Sr, respectievelijk 161sexies en 350a Sr.

De Raad merkt hierbij op dat het onderscheid dat in de Richtlijn wordt gemaakt tussen systeemverstoring en gegevensverstoring in de MvT niet zo scherp tot uitdrukking komt. Enkel artikel 350a Sr ziet namelijk op de opzettelijke en wederrechtelijke aantasting van computergegevens, en de artikelen 138b en 161sexies Sr zijn primair gericht op bescherming van computersystemen. Dit onderscheid in de Richtlijn ware in de MvT te verduidelijken.

De Raad merkt daarnaast op dat terecht wordt voorgesteld het huidige artikel 161sexies Sr aan te passen en over te hevelen naar een nieuw artikel 350c Sr. In de MvT wordt in dit verband gesteld dat de Richtlijn de eis dat het moet gaan om een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst niet stelt, waardoor deze eis in artikel 161sexies Sr dient te komen vervallen. De Raad merkt op dat de Richtlijn spreekt over "informatiesystemen", waaronder volgens artikel 2

wordt verstaan: "*apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken, alsmede de computergegevens die met dat apparaat of die groep van apparaten worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan.*" In de lijn van deze definitie heeft de Richtlijn geen betrekking op de strafbaarstelling van de verstoring van een telecommunicatienetwerk. Het gaat hier namelijk om een systeem waarin computergegevens worden verwerkt, terwijl een telecommunicatienetwerk ziet op het systeem dat overdracht mogelijk maakt van signalen via kabels, radiogolven, optische middelen of andere elektromagnetische middelen (art. 1.1 Telecommunicatiewet), hetgeen breder is dan enkel de overdracht van computergegevens. De Richtlijn stelt aldus niet de eis dat het moet gaan om een telecommunicatienetwerk of –dienst, laat staan of deze openbaar is of niet. Dat dit vereiste van artikel 161sexies Sr aldus moet komen te vervallen verdient dan ook een nadere toelichting.

- **Artikel 9, lid 4 van de Richtlijn**

Het voorgestelde nieuwe derde lid van artikel 138b Sr is een uitwerking van artikel 9, lid 4 van de Richtlijn en benoemt als strafverzwarende omstandigheid het gegeven dat het strafbare feit is gepleegd tegen een informatiesysteem (geautomatiseerd werk) "*van een vitale infrastructuur*".

De Raad merkt op dat het begrip "vitale infrastructuur" in de MvT niet nader wordt gedefinieerd of omschreven, terwijl het evenmin reeds elders in strafrechtelijke wetgeving voorkomt en/of daaromtrent richtinggevende jurisprudentie bestaat. Het verdient daarom aanbeveling een dergelijke nadere definiëring of omschrijving alsnog in de MvT op te nemen. Wellicht kan hierbij aansluiting worden gezocht bij jurisprudentie waarin bijvoorbeeld begrippen zoals 'gegevens ten algemene nutte' en 'gemeen gevaar' worden uitgelegd.

- **Artikel 10 van de Richtlijn**

Artikel 10 van de Richtlijn verplicht – zakelijk weergegeven – de lidstaten onder meer tot het nemen van maatregelen teneinde te verzekeren dat ook rechtspersonen strafrechtelijk verantwoordelijk kunnen worden gehouden voor de in de artikelen 3 tot en met 8 van de Richtlijn genoemde strafbare feiten, indien deze zijn gepleegd ten hunnen voordele door een hunner functionarissen, ook als deze feiten konden worden gepleegd omdat er vanuit de rechtspersoon onvoldoende toezicht of controle op de strafbaar handelende perso(o)n(en) werd gehouden.

De Richtlijn merkt blijkens de omschrijving in artikel 2 onder c van de Richtlijn onder meer niet als rechtspersoon in de zin van de Richtlijn aan: "*overheidsentiteiten die handelen in de uitoefening van het openbaar gezag*". De Raad merkt op dat deze definitie niet geheel lijkt aan te sluiten bij de in de zogenaamde Pikmeer-II jurisprudentie door de Hoge Raad geformuleerde criteria wanneer en onder welke condities publiekrechtelijke personen worden uitgesloten van strafvervolging.[2] In deze jurisprudentie wordt de strafrechtelijke immuniteit van publiekrechtelijke rechtspersonen immers beperkt tot "*gedragingen die naar haar aard en gelet op het wettelijk systeem rechtens niet anders dan door bestuursfunctionarissen worden verricht in het kader van de aan het openbaar lichaam*

[2] HR 6 januari 1998, NJ 1998, 367.

opgedragen bestuurstaak, zodat uitgesloten is dat derden in zoverre op gelijke voet als het openbaar lichaam aan het maatschappelijk verkeer deelnemen."
"Uitoefening van openbaar gezag" lijkt te zien op een breder palet van gedragingen dan die waarop de Hoge Raad in voormelde jurisprudentie het oog heeft. Niet elke uitoefening van openbaar gezag impliceert immers dat het ook gaat om een handeling die – met uitsluiting van derden – aan het betreffende openbare lichaam c.q. de overheid als zodanig is voorbehouden. De conclusie zou dan ook kunnen zijn dat ten aanzien van de in de Richtlijn omschreven (en in het Wetsvoorstel in strafbepalingen omgezette) gedragingen ingevolge het Nederlandse nationale strafrecht eerder strafbare betrokkenheid van publiekrechtelijke rechtspersonen kan worden aangenomen dan uit de Richtlijn zelf voortvloeit. Het verdient daarom aanbeveling in de MvT nader aandacht te besteden aan de vraag of, en zo ja in hoeverre en onder welke condities, wordt beoogd ook Nederlandse publiekrechtelijke rechtspersonen, waaronder begrepen samenwerkingsverbanden tussen deze rechtspersonen (ook als deze plaats vinden in de vorm van privaatrechtelijke rechtspersonen, zoals stichtingen) onder het bereik van de implementatiewetgeving te brengen.

- **De voorgestelde maximale strafbedreigingen en de toepassing van voorlopige hechtenis**

In de MvT wordt geen expliciete aandacht besteed aan de relatie tussen de strafmaxima voor de voorgestelde nieuwe strafbare feiten (c.q. de verhoging daarvan voor een aantal reeds bestaande feiten) en de mogelijke toepassing van voorlopige hechtenis. De Raad stelt vast dat ingevolge het Wetsvoorstel voor de in de artikelen 350c en 350d Sr nieuw omschreven strafbare gedragingen geen voorlopige hechtenis is toegestaan, nu de daarop gestelde maximale strafbedreiging ligt onder de ondergrens van 4 jaar gevangenisstraf als genoemd in artikel 67, lid 1, onder a Sv, en in het Wetsvoorstel niet tevens wordt voorgesteld deze beide bepalingen te doen opnemen in artikel 67, lid 1 onder b Sv. De Raad vraagt zich af of dit geen omissie betreft, aangezien diverse andere cyberdelicten, met eenzelfde of vergelijkbare strafbedreiging als de thans voorgestelde artikelen 350c en 350d Sr, wel zijn genoemd in artikel 67, lid 1, onder b Sv.

Daarnaast merkt de Raad op dat de toepassing van voorlopige hechtenis ten aanzien van de in het Wetsvoorstel genoemde strafbare gedragingen naar verwachting slechts beperkt zal kunnen zijn. Gegeven de aard van de gedragingen, en de daarop in het Wetsvoorstel gestelde maximale strafbedreigingen, zal ingevolge artikel 67a, lid 2 onder 2 en 4 Sv immers alleen een grond voor voorlopige hechtenis aanwezig kunnen worden geacht indien er ernstig rekening moet worden gehouden dat de verdachte (wederom) een misdrijf zal begaan waardoor algemeen gevaar voor goederen kan ontstaan, dan wel zijn voorlopige hechtenis noodzakelijk is voor het, anders dan door verklaringen van de verdachte, aan de dag brengen van de waarheid.

In de rechtsliteratuur wordt aangenomen dat met "misdrijven waardoor algemeen gevaar voor goederen kan ontstaan" wordt gedoeld op de misdrijven welke zijn omschreven in boek 2, titel VII van het Wetboek van Strafrecht. In de onderhavige context is van de in titel VII opgenomen misdrijven alleen artikel 161sexies Sr (indien en voor zover door het al dan niet opzettelijk vernielen/beschadigen van een geautomatiseerd werk tevens gemeen (levens)gevaar voor personen of goederen kon ontstaan) relevant.. De nu voorgestelde leden 2 en 3 van artikel 138b Sr zullen niet in titel VII worden opgenomen, zodat er

twijfel kan bestaan of gevaar voor recidive voor deze feiten als voldoende grond voor de toepassing van voorlopige hechtenis kan gelden.
Ten aanzien van de onderzoeksgrond merkt de Raad op dat bij cybercrimedelicten veelal door middel van het veiligstellen en in beslag nemen van (gegevensdragers met) loggings- en andere data de voor het onderzoek van belang zijnde gegevens al op een vroeg moment uit de invloedssfeer van de verdachte zijn geraakt. Het is dan ook niet vanzelfsprekend dat een verdachte op deze grond in voorlopige hechtenis kan worden genomen dan wel (al dan niet tot aan de zitting) kan worden gehouden.
Het voorgaande brengt met zich dat ook indien bijvoorbeeld sprake is van een verdenking inzake het thans voorgestelde nieuwe 3e lid van artikel 138b Sr en het feit is gepleegd tegen een geautomatiseerd werk behorende tot de vitale infrastructuur (waarbij grote maatschappelijke schade en -onrust kan zijn ontstaan) naar verwachting slechts sprake zal zijn van beperkte mogelijkheden tot toepassing van voorlopige hechtenis. De vraag rijst of zulks bij het opstellen van het Wetsvoorstel c.q. bij het formuleren van de in het Wetsvoorstel gekozen strafmaxima is onderkend. De Raad adviseert hierop in de MvT nader in te gaan.

- **Verzamelen van gegevens**

Op pagina 2 van de MvT wordt in de inleiding gesteld dat er behoefte is aan het verzamelen van vergelijkbare gegevens in Europese landen over de in de Richtlijn bedoelde strafbare feiten. Het woord gegevens wekt op dat moment verwarring omdat het niet duidelijk is of het statistische of persoonsgegevens betreft. Pas bij verdere lezing wordt op pagina 6 MvT duidelijk dat het hier conform artikel 13 en 14 van de Richtlijn inderdaad statistische gegevens betreft. De Raad adviseert dit in de inleiding te verduidelijken.