Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2005–2006

26 671 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

30 036 (R 1784) Goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18)

D

MEMORIE VAN ANTWOORD

Ontvangen 21 februari 2006

Het verheugt mij dat de leden van de commissie met veel belangstelling hebben kennisgenomen van beide wetsvoorstellen. Het komt ook mij praktisch voor, dat de vragen over beide wetsvoorstellen worden gecombineerd. Graag beantwoord ik de in het voorlopig verslag gestelde vragen en ga ik – voor zover daartoe aanleiding is – in op de daarin gemaakte opmerkingen.

Met genoegen constateer ik dat de leden van de CDA-fractie ermee instemmen dat voor de implementatie van het Cybercrime Verdrag is aangesloten bij het reeds aanhangige wetsvoorstel Computercriminaliteit-II. En het verheugt mij dat de leden van de D66-fractie het voorliggende voorstel tot modernisering toejuichen. Met hen meen ik dat het niet wenselijk is dat het Wetboek van Strafrecht en het Wetboek van Strafvordering alleen met kunstmatige ingrepen en met een extensieve interpretatie aansluiting blijven vinden bij de hedendaagse maatschappij.

Artikel 138a Wetboek van Strafrecht

In de commissie leeft twijfel over de wenselijkheid van de nieuwe redactie van het verbod van computervredebreuk in artikel 138a Sr. De commissie onderstreept dat zij voorstander is van een zo strikt mogelijke implementatie van internationaal gemaakte afspraken. Juist in dat verband hecht ik eraan de aandacht nog eens te vestigen op het Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen (PbL 2005/69, blz. 67) – dat bij deze gelegenheid voor zover nog nodig ook geïmplementeerd wordt – in relatie tot het thans geldende artikel 138a Sr. Artikel 2, eerste lid, van het Kaderbesluit verplicht de EU-lidstaten ertoe om de opzettelijke, wederrechtelijke toegang tot een informatiesysteem strafbaar te stellen. Het tweede lid van dat artikel bepaalt: «Iedere lidstaat kan beslissen dat de in lid 1 bedoelde gedragingen alleen strafbaar worden gesteld indien het feit wordt gepleegd door een inbreuk op de beveiligingsmaatregelen». Strikte implementatie van deze bepaling brengt

KST94883
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2006

derhalve met zich mee dat Nederland de keuze heeft tussen twee opties: óf een algehele strafbaarstelling van de opzettelijke en wederrechtelijke toegang tot een informatiesysteem, óf een systeem waarbij als (enige) voorwaarde voor strafbaarheid geldt dat het feit plaatsvindt door een doorbreking van een beveiliging.
De thans geldende Nederlandse bepaling over computervredebreuk, artikel 138a Sr, kent een systematiek die afwijkt van de twee opties die het Kaderbesluit openlaat. De wetgever heeft er in artikel 138a, eerste lid, Sr immers voor gekozen om computervredebreuk strafbaar te stellen indien is voldaan aan één van de in de onderdelen a en b genoemde voorwaarden: (a) indien er enige beveiliging is doorbroken of (b) indien de toegang is verworven door een technische ingreep, met behulp van valse signalen of en valse sleutel dan wel door het aannemen van een valse hoedanigheid. Dat indertijd niét alleen werd gekozen voor het doorbreken van een beveiliging als voorwaarde voor strafbaarheid, had als achtergrond dat uit dat criterium niet duidelijk werd wat onder beveiliging diende te worden verstaan en aan welke eisen die beveiliging zou hebben te voldoen (Kamerstukken II, 21 551, nr. 3, blz. 16). Daarom werd naast onderdeel a ook onderdeel b toegevoegd.

Aangezien de voorwaarde in onderdeel b van artikel 138a, eerste lid, in strijd is met artikel 2 van het Kaderbesluit, moet artikel 138a Sr in ieder geval gewijzigd worden. De keuze ging daarbij in hoofdzaak tussen het schrappen van alleen onderdeel b en het schrappen van beide onderdelen als voorwaarde voor strafbaarheid. In de toelichting bij de tweede nota van wijziging (Kamerstukken II 2004/05, 26 671, nr. 7, blz. 31) heb ik uiteengezet dat ik het onwenselijk achtte om onderdeel b te schrappen en onderdeel a te handhaven, omdat daardoor een strakkere voorwaarde voor strafbaarheid zou komen te gelden dan thans in Nederland het geval is en daardoor het bewijs van het strafbare feit in bepaalde gevallen dus lastiger te leveren zou worden. Daarom heb ik gekozen voor de andere optie die het Kaderbesluit openlaat, te weten een algehele strafbaarstelling van het opzettelijk en wederrechtelijk binnendringen. Om daarbij toch zoveel mogelijk continuïteit met de thans geldende wetsbepaling te bereiken en om de bepaling in de praktijk goed toepasbaar te laten zijn, zijn de elementen die tot nu toe in de onderdelen an en b als voorwaarde voor strafbaarheid zijn gesteld, opgenomen als voorbeelden van gevallen waarbij *in ieder geval* sprake is van binnendringen in de zin van de wet. De aldus tot stand gekomen strafbepaling voldoet zowel aan artikel 2 van het EU-Kaderbesluit als aan artikel 3 van het Cybercrime Verdrag.

Ik hoop met het voorgaande de bedoeling en de achtergrond van de wijziging van artikel 138a Sr te hebben verhelderd en tevens duidelijk gemaakt te hebben dat de kennelijk achterliggende gedachte bij de gestelde vragen, namelijk dat het doorbreken van een beveiliging thans een noodzakelijke (en wel de enige) voorwaarde voor strafbaarheid zou zijn, onjuist is.

Met de leden van de CDA-fractie ben ik van mening dat het van groot belang is en blijft, om de eigen verantwoordelijkheid van gebruikers van de middelen van informatie- en communicatietechniek te benadrukken. Natuurlijk zullen de gebruikers zelf verantwoordelijk zijn voor het zorgvuldig omgaan met de hen ten dienste staande middelen. Dat zulks in het civiele recht een vanzelfsprekendheid is, betekent echter niet dat het strafrecht niet reeds gevolgen kan verbinden aan handelen dat kon plaatsvinden mede doordat het slachtoffer geen – of niet afdoende – feitelijke beveiligingsmaatregelen had getroffen. Het door deze leden genoemde voorbeeld van de inboedelverzekering kan dit verhelderen. De meeste inboedelverzekeringen zullen inderdaad als clausule hebben dat slechts tot uitkering wordt overgegaan indien sprake was van (in)braak. Dat laat

onverlet dat het Wetboek van Strafrecht van oudsher in artikel 138 huisvredebreuk strafbaar stelt ook zonder dat sprake hoeft te zijn van braak etc. (zie artikel 138 Sr). Van wederrechtelijk binnendringen in een woning kan dan ook reeds sprake zijn indien iemand een woning binnengaat tegen de verklaarde wil van de bewoner, zonder dat de woning adequaat is afgesloten (zie ook Handelingen II 13 september 2005, blz. 105–6357, m.k.). Indien evenwel sprake is van braak, hoeft verder niet bewezen te worden dat sprake was van «binnendringen», zo stelt het tweede lid van artikel 138. Braak is derhalve geen voorwaarde voor strafbaarheid, maar vergemakkelijkt het bewijs van «binnendringen». Een min of meer gelijke constructie wordt thans gekozen in het voorgestelde artikel 138a Sr.

De leden van de fracties van VVD en PvdA merken terecht op dat zowel het Verdrag van de Raad van Europa als het Kaderbesluit van de Raad van de Europese Unie inzake aanvallen op informatiesystemen de wetgever ruimte laten om de strafbaarstelling van computervredebreuk te beperken tot gevallen waarin het feit wordt gepleegd door het doorbreken van een beveiliging. Ik heb dan ook de mogelijkheid overwogen om van deze beperkingsmogelijkheid gebruik te maken. Zoals ik hierboven al aangaf, was bij die optie echter het probleem dat in dat geval computervredebreuk niet meer strafbaar zou zijn als er geen beveiliging was doorbroken maar de toegang (slechts) was verworven door een technische ingreep, met hulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid. Het Kaderbesluit biedt immers slechts de keuze tussen een algehele strafbaarstelling van onrechtmatige toegang tot een informatiesysteem en een strafbaarstelling waarbij alleen de beperking wordt aangebracht dat het feit dient plaats te vinden door een doorbreking van een beveiliging. Door te kiezen voor deze laatste modaliteit zou worden afgedaan aan de strafrechtelijke bescherming die thans wordt geboden door artikel 138a Sr. Daarom heb ik gekozen voor een oplossing die enerzijds voorziet in een algeheel verbod op het opzettelijk en wederrechtelijk binnendringen in een computer maar die anderzijds zorgt voor continuïteit met het huidige artikel 138a Sr door de daarin opgenomen modaliteiten (doorbreken van een beveiliging; technische ingreep; valse signalen; valse sleutel; valse hoedanigheid) uitdrukkelijk te vermelden als gevallen waarin *in ieder geval* sprake is van binnendringen.

De leden van genoemde fracties hebben voorbeelden gevraagd van situaties waarin gesproken kan worden van het opzettelijk (en) wederrechtelijk binnendringen zonder dat daarbij tevens enige beveiliging wordt doorbroken of omzeild. Ten eerste noem ik de gevallen waarin – in de terminologie van het huidige artikel 138a – gebruik is gemaakt van valse signalen of een valse hoedanigheid of waarbij een technische ingreep is gehanteerd die niet als doorbreking van een beveiliging kan worden aangemerkt. Denkbaar is evenwel dat zich ook daarbuiten situaties kunnen voordoen waarin sprake is van opzettelijk en wederrechtelijk binnendringen in een computer(systeem). Het enkele gebruikmaken van een voor algemeen gebruik bestemde computer zal natuurlijk niet als wederrechtelijk binnendringen aangemerkt worden. Als men zich daarentegen bijvoorbeeld na een fysieke inbraak in een woning toegang verschaft tot een zich in die woning bevindende computer, zal daarbij van computervredebreuk sprake kunnen zijn – een situatie waarvan het de vraag is of die door de huidige wetsbepaling wordt gedekt. Iets dergelijks is denkbaar indien iemand zich toegang verschaft tot een computer terwijl dat hem uitdrukkelijk is verboden. Of er bij het «enkele passeren» van een virtueel bordje «verboden toegang» al sprake zal zijn van opzettelijk en wederrechtelijk binnendringen, zal afhangen van de omstandigheden. De leden van de genoemde fracties hebben in dit verband in herinnering geroepen dat een belangrijke reden voor de formulering van het huidige artikel 138a Sr was gelegen in de kenbaarheid voor de potentiële dader. In de woorden

van deze leden: de potentiële dader moet weten dat hij zich op verboden terrein gaat begeven. Ook in de nieuwe formulering van 138a Sr zal voor de potentiële dader kenbaar moeten zijn dat hij zich op verboden terrein gaat begeven. Met andere woorden: de wederrechtelijkheid van zijn handelen zal voor hem kenbaar moeten zijn. Ik wijs er daarbij echter wel op dat – als spiegelbeeld van de verantwoordelijkheid van de beheerder c.q. gebruiker van een computersysteem – ook de dader van zijn kant een maatschappelijke verantwoordelijkheid heeft, namelijk om af te zien van het binnendringen in een computersysteem indien hij daartoe niet bevoegd is. Dat is immers het kenmerkende element van computervredebreuk.

Alles afwegende meen ik dat de voorgestelde bepaling van artikel 138a voldoet aan zowel het Verdrag als het Kaderbesluit en bovendien het voordeel heeft dat er wordt aangesloten bij de sinds 1993 bekende bestanddelen zonder de reikwijdte van de bepaling in te perken.

De commissie stelde in dit verband nog de vraag of door de voorgestelde tekst van artikel 138a Sr de formulering van computervredebreuk in de verdragssluitende landen niet zeer uiteen zal gaan lopen, waarbij zij ook een verband legde met de verschillen tussen de Franse en de Engelse tekst van het Cybercrime Verdrag.
Aangenomen mag worden dat door de implementatie van het Cybercrime Verdrag én door de implementatie van het EU-Kaderbesluit onmiskenbaar juist een grotere eenheid zal ontstaan door het enkele feit dat in alle aangesloten landen computervredebreuk als zodanig strafbaar gesteld dient te worden. Dat zich daarbij verschillen in formulering zullen voordoen is onvermijdelijk. De doelstelling van het Cybercrime Verdrag en het EU-Kaderbesluit is niet om te komen tot uniformiteit in strafbepalingen, maar om een bepaalde ondergrens te bereiken in datgene wat als strafwaardig gedrag wordt aangemerkt. Het hangt doorgaans overigens meer af van de nationale wetgevingstradities dan van de exacte redactie van internationale rechtsinstrumenten, hoe nationale bepalingen luiden. Ook na de implementatie van het Verdrag door de verdragssluitende partijen zullen er dus verschillen blijven bestaan in de formulering van de nationale wetgeving. Daarbij moet bovendien bedacht worden dat zowel het Cybercrime Verdrag als het EU-Kaderbesluit de Staten uitdrukkelijk de mogelijkheid biedt om te kiezen voor de ene of de andere modaliteit: het EU-Kaderbesluit laat, zoals hiervoor uiteengezet, de keus tussen een algeheel verbod en een verbod met als voorwaarde dat een beveiliging is doorbroken; het Cybercrime Verdrag laat een zelfs nog grotere schakering toe. Volledige harmonisatie is dus uitdrukkelijk niet nagestreefd.

Wat betreft de vraag over de verschillen tussen de Franse en de Engelse tekst van het Verdrag merk ik het volgende op. Ik neem aan dat de commissie hierbij doelt op de kwestie die in de toelichting op de tweede nota van wijziging (Kamerstukken II 2004–05, 26 671, nr. 7, blz. 33) aan de orde was naar aanleiding van de vraag in het advies van de NVvR, of de oorspronkelijke tekst van artikel 138a Sr («opzettelijk wederrechtelijk» zonder tussenvoeging van het woord «en» zoals toegevoegd in het wetsvoorstel) niet beter zou aansluiten bij artikel 2 van het Verdrag. In reactie daarop gaf ik aan dat voor een interpretatie van artikel 2 van het Verdrag zoals kennelijk door de NVvR gelezen – in die zin dat de opzet ook gericht zou moeten zijn op de wederrechtelijkheid als zodanig – weliswaar *wellicht* een aanknopingspunt te vinden zou kunnen zijn in de Engelse tekst van de bepaling, maar dat het Explanatory Memorandum daarvoor toch geen aanwijzingen gaf, terwijl bovendien de Franse tekst helderheid bood door te spreken over «intentionnel *et* sans droit». Ik voeg daar nog aan toe dat ook de Engelse tekst bij nadere beschouwing geen aanknopingspunt biedt voor de interpretatie zoals kennelijk door de NVvR

gelezen. Het opzet-bestanddeel in de Engelse tekst is immers geplaatst tussen komma's, direct voorafgaand aan de handeling waarop het betrekking heeft, namelijk «the access». De gesuggereerde interpretatie zou hout snijden indien in de Engelse tekst de woorden «without right» direct na «the access» zouden zijn geplaatst. Alles afwegende meen ik dat het verschil in redactie tussen beide teksten niet mag worden geïnterpreteerd als een materieel relevant verschil tussen de twee authentieke Verdragsteksten maar eerder als een technisch verschil in redactie.

Ten aanzien van het toevoegen van het woord «en» tussen «opzettelijk» en «wederrechtelijk» merkten de leden van de CDA-fractie nog op dat de in de memorie van toelichting gegeven motivering niet concludent is. In het in de toelichting gegeven voorbeeld is, zo stellen zij, duidelijk dat de opzet op de wederrechtelijkheid is gericht, zodat daar geen sprake is van een onnodig zware eis. In het in de memorie van toelichting gegeven voorbeeld was inderdaad sprake van een situatie waarin «wetenschap van het wederrechtelijke van zijn handelen (mag) worden verondersteld» (Kamerstukken II 1998–99, 26 671, nr. 3, blz. 44), zodat aangenomen mag worden dat de opzet ook op de wederrechtelijkheid als zodanig gericht was. Niettemin meen ik dat de voorgestelde wetswijziging zinvol is omdat daarmee zeker wordt gesteld dat in de telastelegging niet hoeft te worden gesteld en vervolgens bewezen hoeft te worden verklaard dat de opzet ook op de wederrechtelijkheid betrekking had.

Deze leden hebben nog aandacht gevraagd voor de positie van «onhandige gebruikers», die toevallig een verkeerd nummer intoetsen en dan in het systeem van een onbeveiligde gebruiker binnenkomen. Ook bij de nieuwe bepaling zullen dergelijke gevallen buiten de sfeer van het strafrecht blijven: de opzet op het binnendringen als zodanig ontbreekt immers.

Met het vorenstaande hoop ik voldoende aangegeven te hebben dat er, het Cybercrime Verdrag en het Kaderbesluit in onderlinge samenhang bezien en met inachtneming van de wens van een minimaal gelijkblijvend niveau van strafrechtelijke bescherming tegen computervredebreuk, goede grond is om artikel 138a Sr te wijzigen zoals in het wetsvoorstel is voorgesteld.

Tenslotte heeft de commissie nog mijn reactie gevraagd op de suggestie om, met gebruikmaking van artikel V van wetsvoorstel CC-II, de wijziging van artikel 138a Sr niet in werking te laten treden. Ik stel hierbij graag voorop dat een inwerkingtredingsbepaling zoals opgenomen in artikel V van het wetsvoorstel niet is bedoeld om een of meer onderdelen van de wet in het geheel niet in werking te laten treden, maar alleen om daarvoor zonodig verschillende tijdstippen te kiezen. De tekst van artikel V omvat immers de norm «De artikelen van deze wet treden in werking». Maar afgezien daarvan meen ik met het voorgaande voldoende duidelijk te hebben gemaakt dat zonder wijziging van artikel 138a Sr onze wetgeving niet zou voldoen aan artikel 2 van het EU-Kaderbesluit, terwijl met de voorgestelde wijziging tevens wordt tegemoet gekomen aan de wenselijkheid van een strafrechtelijk adequaat beschermingsniveau tegen computervredebreuk.

Enkele definitievragen

De leden van de D66-fractie vroegen zich af of het onderscheid tussen stromende en opgeslagen gegevens nog wel noodzakelijk is. Zoals deze leden terecht opmerkten, levert dit onderscheid een bijdrage aan de precisering van bevoegdheden van de opsporingsautoriteiten. Aan de andere kant vroegen zij zich af of met de toenemende integratie van telefonie en

internet het onderscheid nog wel nut heeft. Graag geef ik deze leden toe dat het onderscheid tussen stromende en opgeslagen gegevens steeds minder relevant wordt en, mede gelet op de steeds verdergaande digitalisering van gegevensoverdracht, ook steeds lastiger te bepalen. Het in het strafrecht zo centrale legaliteitsbeginsel eist evenwel dat zowel strafbepalingen als strafvorderlijke bevoegdheden zo nauwkeurig mogelijk worden omschreven, maar gelet op het vorenstaande kan het dan wel nodig zijn om in bepaalde gevallen ervoor te zorgen dat de beide situaties – stromend én opgeslagen – door de wet worden gedekt. Daarom voorziet het wetsvoorstel op een aantal plaatsen in aanvulling van bepalingen waarin tot nu toe een beperking besloten ligt tot opgeslagen gegevens (zie bijvoorbeeld de wijzigingen van artikel 138a, tweede lid, en 161sexies, eerste lid, Sr).
De leden van de D66-fractie vroegen specifiek, of een sms-chatsessie stromend is of dat het daarbij gaat om telkens opnieuw opgeslagen gegevens. De vraag, zo gesteld, is niet ondubbelzinnig te beantwoorden. In de fase van de gegevensoverdracht van de zender naar de ontvanger is in ieder geval sprake van stromende gegevens, maar afhankelijk van de gebruikte techniek is er tevens op een of meer momenten sprake van – al of niet zeer kort durende – opslag van gegevens. De strafvorderlijke bevoegdheid van «opnemen» (aftappen) kan worden ingezet voor de gegevensoverdracht als zodanig. De bevoegdheid van het vorderen van gegevens kan worden ingezet voor het verkrijgen van de opgeslagen gegevens. Zo'n vordering van opgeslagen gegevens kan worden gericht tot degene van wie redelijkerwijs kan worden aangenomen dat hij toegang heeft tot de gegevens, met uitzondering van de verdachte. In dat verband is van belang dat de gegevens van een sms-chat doorgaans niet worden opgeslagen in het netwerk van de telecommunicatieaanbieder, maar (eventueel zeer kortdurend) in het geheugen van de (mobiele) telefoon(s). Tenslotte is in dit opzicht nog van belang de nieuwe bevoegdheid inzake bevriezing van vluchtige gegevens (artikel 126ni Sv). Ook die vordering kan overigens niet worden gericht tot de verdachte. Voor zover behoefte bestaat aan kennisneming van de opgeslagen gegevens zoals deze zich bevinden in het geheugen van de mobiele telefoon van de verdachte, komt – zonodig in aanvulling op het opnemen van de gegevensstroom als zodanig – inbeslagneming van de mobiele telefoon in aanmerking.

Deze leden stelden ten slotte enkele vragen over het begrip e-mail. E-mail wordt in het algemeen gebruikt als een verzamelterm voor diensten waarbij elektronische berichten van een afzender naar een ontvanger worden getransporteerd (zie ook Kamerstukken II 2004/05, 26 671, nr. 10, blz. 21). De transportfase omvat mede de opslag van e-mailberichten in de zogenaamde mailbox van de provider, waar de berichten aanwezig blijven tot ze door de ontvanger worden geopend en naar diens computersysteem worden overgebracht. Providers vervoeren allerlei soorten berichten, bestanden en gegevens, waaronder ook sms-berichten en MSN-berichten. Onder de transportfase valt niet meer de opslag van – bijvoorbeeld – de geschiedenis van MSN-verkeer in het computersysteem van de ontvanger.

De leden van de fracties van VVD en PvdA vroegen of de definities van «gegevens» en «geautomatiseerd werk», die zijn opgenomen in het Wetboek van Strafrecht, niet ook opgenomen dienen te worden in het Wetboek van Strafvordering. De definitiebepalingen van deze begrippen zijn destijds door middel van een amendement alleen in het Wetboek van Strafrecht opgenomen. Uit de praktijk is mij evenwel niet bekend dat er problemen zijn ontstaan doordat een aparte definitiebepaling in het Wetboek van Strafvordering ontbreekt. De begrippen worden kennelijk

gehanteerd in de betekenis die daarin is gegeven in de definitiebepalingen in het Wetboek van Strafrecht.

Vragen met betrekking tot bevoegdheden

Het verheugt mij dat de leden van de CDA-fractie met instemming kennis hebben genomen van de passage over artikel 8 van het EVRM. Zij vroegen zich af waarom slechts bij een gedeelte van de nieuwe bevoegdheden tot het uitoefenen van dwangmiddelen sprake is van toezicht op het gebruik daarvan door de rechter-commissaris. De reden is dat hierbij – zoals ook voorgeschreven wordt door artikel 15 van het Cybercrime Verdrag – aansluiting is gezocht bij ons bestaande stelsel van strafvorderlijke bevoegdheden, dat op zichzelf voldoet aan de eisen van artikel 8 EVRM. De Nederlandse strafvordering kent een oplopende schaal van bevoegdheden, te beginnen bij bevoegdheden die iedere burger mag toepassen (aanhouding van een verdachte bij ontdekking op heterdaad – artikel 53 Sv) en eindigend bij bevoegdheden die slechts mogen worden toegepast door of met machtiging van de rechter-commissaris of door de zittingsrechter. Bepalend daarvoor is vooral de inbreuk die de bevoegdheidstoepassing maakt op fundamentele rechten van betrokkene. Bij de toepassing van artikel 126m of 126t Sv gaat het om het opnemen van communicatie en het kennisnemen van de inhoud daarvan. Dat zijn ingrijpende bevoegdheden, om welke reden er destijds voor gekozen is de toepassing daarvan te binden aan een voorafgaande machtiging van de rechter-commissaris. Bij de artikelen 126n en 126u gaat het daarentegen om het vorderen van verkeersgegevens omtrent een gebruiker, wat een geringere inbreuk op fundamentele rechten betekent. De wetgever heeft ervoor gekozen deze bevoegdheid toe te delen aan de officier van justitie. Bij de thans nieuw voorgestelde bevoegdheid van artikel 126ni Sv (de zogenaamde bevriezingsbevoegdheid) gaat het om een vordering, gericht tot een aanbieder, om bepaalde gegevens tijdelijk te bewaren en beschikbaar te houden; de vordering biedt geen grondslag voor kennisneming van de inhoud van de aldus bewaarde en beschikbaar gehouden gegevens. Om die reden is de inbreuk minder vergaand dan die van artikel 126m Sv en zelfs minder vergaand dan die van artikel 126n Sv. Daarom heb ik ervoor gekozen de toepassing van de bevoegdheid niet afhankelijk te stellen van een machtiging door de rechter-commissaris maar de bevoegdheid te leggen bij de officier van justitie. Aanvankelijk heb ik overwogen de bevoegdheid, gelet op het beperkte inbreukmakende karakter ervan, te leggen bij de hulpofficier van justitie maar naar aanleiding van de daarop gegeven adviezen heb ik uiteindelijk gekozen voor de officier van justitie.

De genoemde leden hebben nog gevraagd of niet valt te vrezen dat in de praktijk de officier van justitie zijn zelfstandige bevoegdheden (in vergaande mate) zal delegeren, zodat de bevoegdheden de facto door hulpofficieren of zelfs – via subdelegatie – door lagere politiefunctionarissen zullen worden uitgevoerd. Deze vrees is ongegrond. In artikel 126, eerste lid, van de Wet op de rechterlijke organisatie is namelijk vastgelegd dat de uitoefening van bevoegdheden van de officier van justitie alleen kan worden opgedragen aan andere bij het parket werkzame ambtenaren, en politieambtenaren vallen niet in die categorie (zie de toelichting op artikel 126 Wet RO in Kamerstukken II 1996–97, 25 392, nr. 3, blz. 41), dus ook de hulp-officier van justitie niet. Overigens hoeft bij de hier aan de orde zijnde bevoegdheden ook niet gevreesd te worden voor mandaatverlening aan de wél bij het parket werkzame ambtenaren, aangezien artikel 126, derde lid, Wet RO bepaalt dat mandaatverlening niet is toegelaten indien de regeling waarop de bevoegdheid steunt of de aard van de bevoegdheid zich daartegen verzet. Volgens artikel 126, derde lid, Wet RO is daarvan in elk geval sprake voor zover het gaat om de

toepassing van dwangmiddelen als bedoeld in Titel IV van het Eerste Boek Sv. Gelet op de inhoud van de bevoegdheden, geregeld in Titel IVA van het Eerste Boek Sv, moet geconcludeerd worden dat ook de aard van die bevoegdheden zich verzet tegen mandaatverlening.

De leden van de D66-fractie vroegen of het te verwachten is dat het OM interne beleidsregels zal opstellen voor de wijze waarop gebruik wordt gemaakt van de bevoegdheid om gegevens die tijdens een doorzoeking in een geautomatiseerd werk worden aangetroffen, in beslag te nemen. Ik neem aan dat hiermee gedoeld wordt op hetzij de bevoegdheid om *gegevens ontoegankelijk* te maken, hetzij op de bevoegdheid om de *gegevensdrager in beslag te nemen, hetzij op de bevoegdheid om gegevens in het kader van een doorzoeking vast te leggen.* In de nota naar aanleiding van het verslag van de Tweede Kamer (Kamerstukken II 2004/05, 26 671, nr. 10, blz. 11 e.v.) ben ik ingegaan op de verschillende situaties die zich kunnen voordoen. Daarbij heb ik aangegeven dat de beginselen van proportionaliteit, subsidiariteit en effectiviteit steeds in iedere casuspositie goed in acht moeten worden genomen. Mét de vragenstellers ben ik graag eens dat willekeur bij het gebruik van (ook) de hier bedoelde bevoegdheden moet worden voorkomen. Veelal zal het ontoegankelijk maken van bepaalde gegevens een mindere belasting voor de belanghebbenden betekenen dan de inbeslagneming van de gegevensdrager, zodat in die gevallen uit een oogpunt van subsidiariteit en proportionaliteit in beginsel voor die eerste optie gekozen zal moeten worden, althans indien daarmee in voldoende mate kan worden bereikt wat men voor ogen heeft. Steeds is dus een op de specifieke casus toegespitste besluitvorming en belangenafweging vereist, waarbij wel steeds voorop staat dat de toegepaste maatregel in het belang van het onderzoek kan worden geacht. De af te wegen belangen en aspecten kunnen zeer divers zijn, al naar gelang de feiten en omstandigheden van het geval. Zo kan een rol spelen of de kring van degenen die belang hebben bij de gegevens, dezelfde is als de kring van verdachten in het opsporingsonderzoek. Dat zal bij een enkele computer anders liggen dan bij een netwerk. Daarnaast kan bijvoorbeeld ook de complexiteit van de computer of het computersysteem een rol spelen, de daarin vermoedelijk gebruikte programmatuur en dergelijke. Algemene beleidslijnen zullen hiervoor, naar ik meen, moeilijk kunnen worden uitgezet.

Deze leden vroegen tenslotte nog of het wel in het takenpakket van de rechter-commissaris valt, om strafbare feiten te voorkomen. Zoals ik ook al heb aangegeven in de nota naar aanleiding van het verslag van de Tweede Kamer (Kamerstukken II 2004/05, 26 671, nr. 10, blz. 15), behoort het voorkomen en beëindigen van strafbare feiten niet tot de reguliere taken van de rechter-commissaris. Maar dat laat onverlet dat het wenselijk is om de rechter-commissaris de bevoegdheid te verlenen om – binnen het kader van een gerechtelijk vooronderzoek overeenkomstig het voorgestelde artikel 125o Sv – te bepalen dat gegevens ontoegankelijk worden gemaakt voor zover dit nodig is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Het ontoegankelijk maken van gegevens is een maatregel die onlosmakelijk verbonden is met het doorzoeken van een geautomatiseerd werk. Indien dat doorzoeken plaatsvindt in het kader van een gerechtelijk vooronderzoek, is de rechter-commissaris daarvoor verantwoordelijk. Deze dient dan ook verantwoordelijkheid te kunnen dragen voor de maatregel van ontoegankelijkmaking van gegevens, al was het maar omdat die maatregel invloed kan hebben op het onderzoek zelf. Daarom acht ik het wenselijk dat de rechter-commissaris bevoegd is tot het bevelen van de ontoegankelijkmaking tijdens een gerechtelijk vooronderzoek. Ik verwacht overigens wel dat het initiatief daartoe doorgaans zal uitgaan van de officier van justitie.

Bevriezing

De leden van de CDA-fractie hebben gevraagd hoe met betrekking tot de bevoegdheid tot bevriezing kan worden gewaarborgd, dat de integriteit van de gegevens tijdens de bevriezingsperiode niet zal worden aangetast. Formeel staat voorop, dat degene tot wie de vordering tot bevriezing wordt gericht, verplicht is te zorgen dat de gegevens bewaard en beschikbaar gehouden worden in de staat waarin ze verkeren ten tijde van de vordering. Hij mag ten aanzien van de gegevens geen andere bewerking plegen dan nodig om ze te bewaren en beschikbaar te houden. De vordering strekt immers tot het bewaren en beschikbaar houden van gegevens die op zichzelf nu juist vatbaar zijn voor verlies of wijziging. De betrokken persoon of instelling dient dus in te staan voor de integriteit van de gegevens (zie ook Kamerstukken II 2004/05, 26 671, nr. 7, blz. 45). Degene die in dit opzicht onvoldoende gevolg geeft aan de vordering, is strafbaar op grond van artikel 184 Sr (niet opvolgen bevel of vordering). Maar daarmee is nog niet de vraag beantwoord hoe in de praktijk moet worden omgegaan met het bewaken van de integriteit van de desbetreffende gegevens. Zoals ik eerder heb aangegeven naar aanleiding van opmerkingen van het Overlegorgaan Post en Telecommunicatie (idem, blz. 46), ligt het in de rede dat in algemene zin afspraken worden gemaakt tussen het openbaar ministerie en de branche over de wijze waarop dergelijke vorderingen ten uitvoer moeten worden gelegd en, in dat verband, over de inspanningen (bijvoorbeeld het afzonderen van de gewone bedrijfsvoering) die gevergd kunnen worden om vernietiging of aantasting van de gegevens tegen te gaan. Gelet op de eisen van proportionaliteit en subsidiariteit zullen geen onevenredige inspanningen mogen worden verlangd van degenen tot wie vorderingen worden gericht. Zo zal het in het belang van alle partijen zijn om de periode waarvoor het bevriezingsbevel geldt, zo kort mogelijk te stellen.

De leden van de D66-fractie hebben mij gevraagd of ik denk dat de nieuw voorgestelde bevriezingsbevoegdheid (artikel 126ni Sv) een betere oplossing is dan het plan om een algemene bewaarplicht van een of twee jaar te creëren. Zoals ik ook in ander verband – ik verwijs onder meer naar mijn brieven van 6 april en 5 oktober 2005 aan de Eerste Kamer (Kamerstukken I 2004–05, 23 490, AM, blz. 10 en 2005–2006, 23 490, AX, blz. 7) – heb uiteengezet, zijn de doelstellingen van de beide bevoegdheden verschillend. De essentie van de in het ontwerp-kaderbesluit voorziene bewaarplicht is, dat er op het moment van het bewaren van de gegevens geen vermoeden of wetenschap hoeft te bestaan van de later op te sporen strafbare feiten. Daarin onderscheidt de voorgestelde bewaarplicht («retention») zich van de verplichting tot bevriezing («preservation»). De bevriezing van verkeersgegevens heeft uitsluitend effect voor de toekomst en biedt onvoldoende mogelijkheden om de structuur van criminele netwerken in kaart te brengen, nadat de strafbare feiten zijn gepleegd. Opgemerkt zij nog dat de in artikel 126ni Sv voorgestelde bevriezingsbevoegdheid, anders dan de in het ontwerp-kaderbesluit voorziene bewaarplicht, niet is beperkt tot verkeersgegevens. Ik meen dan ook dat aan de beide bevoegdheden, bezien vanuit het perspectief van de behoefte van de opsporing, zelfstandige betekenis toekomt en dat zij elkaar voor een deel kunnen aanvullen. Inmiddels hebben de Europese Raad, de Europese Commissie en het Europees Parlement overeenstemming bereikt over een Richtlijn voor de bewaring van telecommunicatie verkeersgegevens. In de Richtlijn wordt de lidstaten de verplichting opgelegd om te komen tot wetgeving die waarborgt dat bepaalde categorieën van gegevens worden bewaard gedurende een periode van minimaal zes maanden en maximaal twee jaar.

Encryptie

De leden van de D66-fractie hebben aandacht gevraagd voor de medewerkingsplicht bij het ontsleutelen van versleutelde gegevens. Zij vroegen of de geldigheid van het bewijs beïnvloed kan worden door het feit dat gegevens alleen maar door een derde zijn te ontsleutelen. Het enkele feit dat bepaalde gegevens alleen door of met medewerking van een derde te ontsleutelen zijn, heeft op zichzelf geen bijzondere gevolgen voor de *geldigheid* van het bewijs. Waar het om gaat, is of de rechter wettig en overtuigend bewezen acht dat het telastegelegde feit door de verdachte is begaan. Als daartoe gebruik wordt gemaakt van gegevens die door middel van ontsleuteling begrijpelijk zijn geworden, zal de rechter impliciet of expliciet ook een oordeel hebben over de wijze waarop die ontsleuteling heeft plaatsgevonden en in dat verband eventueel ook over de betrouwbaarheid van de handelingen en verklaringen van de persoon of personen die daaraan medewerking hebben verleend. Iets dergelijks geldt in feite ook steeds bij verklaringen van getuigen en deskundigen.
Deze leden vroegen in dit verband ook hoe opsporingsambtenaren zeker kunnen weten dat de gegevens door de derde juist zijn ontcijferd en dat de derde niet een medeverdachte is, en hoe de advocaat van de verdachte kan nagaan of de gegevens wel juist zijn ontcijferd. In de nota naar aanleiding van het verslag van de Tweede Kamer (Kamerstukken II 1004/05, 26 671, nr. 10, blz. 17) heb ik aangegeven dat wanneer er vrees bestaat dat de derde bij ontsleuteling de gegevens zal manipuleren, de opsporingsdiensten de nodige maatregelen kunnen treffen om manipulatie te voorkomen. Ook kan, als een dergelijk risico aanwezig wordt geacht, gevraagd worden om de kennis ter beschikking te stellen waarna door de politie zelf wordt ontsleuteld (artikel 125k, eerste lid, slot). Ik voeg daaraan wel als praktisch argument toe dat het doorgaans snel opvalt als getracht wordt een versleuteld bericht met een verkeerde «sleutel» te ontsleutelen: in dat geval is het bericht doorgaans namelijk gewoon onbegrijpelijk of niet eens leesbaar. De vraag naar de betrouwbaarheid van een derde speelt overigens niet alleen bij het bevel tot ontsleuteling. Ook bij uitlevering van voorwerpen door derden op grond van artikel 96a Sv dienen de opsporingsdiensten zich te vergewissen van de betrouwbaarheid van de uitgeleverde voorwerpen.
De raadsman van de verdachte, tenslotte, krijgt de beschikking over dezelfde informatie als de rechter.

De leden van de CDA-fractie hebben gevraagd of ik kan mededelen, welke positie de meeste andere EU-landen innemen bij het al of niet aan de verdachte kunnen opleggen van een verplichting tot medewerking aan de ontsleuteling van versleutelde gegevens, met name Frankrijk en het Verenigd Koninkrijk. Het betreft de bevoegdheden, neergelegd in artikel 19, vierde lid, van het Cybercrime Verdrag. In het vijfde lid van dat artikel is uitdrukkelijk bepaald dat bij de implementatie van deze bevoegdheden de waarborgen van artikel 15 van het Verdrag in acht moeten worden genomen. Dat betekent dat de bevoegdheden onderworpen moeten worden aan de voorwaarden en waarborgen van het nationale recht, dat tenminste voorziet in een adequate bescherming van de rechten van de mens. In nummer 147 van het Explanatory Memorandum bij het Verdrag is voor zover hier relevant gesteld dat «safeguards that should be addressed under domestic law include the right against self-incrimination». Ik ga er derhalve vanuit dat ook in de andere Europese landen de medewerkingsverplichting niet aan de verdachte kan worden opgelegd. Hoe een en ander vorm krijgt in de nationale wetgeving van de meeste andere EU-landen is nog niet te zeggen, aangezien tot nu toe pas zes EU-landen (Cyprus, Denemarken, Estland, Frankrijk, Hongarije en Litouwen) het Verdrag hebben geratificeerd. Zodra ik heb vernomen hoe

het onderwerp met name in Frankrijk en het Verenigd Koninkrijk is geregeld, zal ik uw Kamer daarvan op de hoogte stellen.

Handhavingsaspecten

De leden van de CDA-fractie gaven aan dat de capaciteit voor handhaving veel aandacht vraagt. Zij vroegen zich in dat verband af of met de start van het National High Tech Crime Centre (NHTCC), de mogelijke inbreng van het Nederlands Forensisch Instituut (NFI) en de aanwezige kennis bij de politieorganisatie zelf voldoende wordt bijgedragen aan de ontwikkeling van een daadwerkelijke bestrijding van computercriminaliteit. Wat betreft het NHTCC merk ik op dat de eindrapportage over dit project binnenkort wordt verwacht en dat het kabinet op basis daarvan een standpunt zal innemen over de verdere organisatorische inbedding van de op nationaal niveau gewenste kennis en taakuitvoering ter zake van de opsporing en vervolging van de hier bedoelde criminaliteit.
De doelstellingen van het kabinet zijn er inderdaad op gericht dat de rechtshandhaving op het terrein van computercriminaliteit voldoende aandacht krijgt. Zoals ik heb uiteengezet in de nota naar aanleiding van het verslag van de Tweede Kamer (Kamerstukken II 2004/05, 26 671, nr. 10, blz. 29 e.v.) is er veel voor nodig om op dit terrein adequaat te kunnen (blijven) optreden. Allereerst gaat het om het op niveau brengen van de kennis en vaardigheden van de huidige rechercheurs om de veel voorkomende vormen van criminaliteit waarbij sprake is van het gebruik van ICT, te kunnen aanpakken. Daarnaast worden specialisten opgeleid voor de meer ingewikkelde vormen van ICT-criminaliteit. Deze verbreding en verdieping van kennis over ICT-criminaliteit binnen de Nederlandse politie vindt plaats door middel van het Landelijk Project Digitaal Opsporen van de Raad van Hoofdcommissarissen, dat moet zijn geïmplementeerd in 2008. Door deze aanpak zal de politie steeds beter in staat zijn om bestaande en nieuwe vormen van criminaliteit op dit terrein op te sporen. Op nationaal niveau wordt in samenspraak met de relevante partners (zowel privaat als publiek) op het gebied van de bestrijding van ICT-criminaliteit gewerkt aan de inrichting van adequate voorziening bij het Korps Landelijke Politiediensten. Op nationaal niveau zal ook worden zorggedragen voor de internationale contacten en voor het bieden van ondersteuning aan (boven)regionale teams.

De leden van de CDA-fractie hebben aandacht gevraagd voor de relatief lage aangiftebereidheid bij slachtoffers. Dat is inderdaad een belangrijk punt, dat vooral ook speelt bij het bedrijfsleven. Zoals ik ook aangaf in de eerder genoemde nota naar aanleiding van het verslag van de Tweede Kamer (id, blz. 3) liggen hieraan in hoofdzaak twee oorzaken ten grondslag, nl. de vrees voor imagoschade bij het betrokken bedrijfsleven en het feit dat voor het opnemen van een aangifte op dit specialistische gebied niet bij iedere opsporingsambtenaar de daarvoor noodzakelijke kennis aanwezig is. Wat betreft het kennisniveau verwijs ik ernaar dat door de hierboven aangegeven ontwikkelingen de politie zowel op regionaal niveau als op landelijk niveau beter in staat zal zijn om aangiften op dit terrein adequaat op te nemen. Wat betreft de vrees voor imagoschade merk ik op dat – zoals ook in zojuist genoemde nota werd vermeld – door het Nationaal Platform Criminaliteitsbeheersing een project Aanpak Cybercrime is gestart dat onder andere tot doel heeft een betere vertrouwensrelatie tussen opsporingsinstanties en bedrijfsleven te bewerkstelligen ter verbetering van de onderlinge samenwerking. De projectgroep heeft inmiddels een plan van aanpak gepresenteerd, dat door het Nationaal Platform Criminaliteitsbestrijding is geaccordeerd en onder verantwoordelijkheid van de staatssecretaris van Economische Zaken wordt uitgevoerd. Doelstelling hiervan is onder meer dat bij het bedrijfsleven de bereidheid zal toenemen om aangifte te doen.

Tenslotte vroegen de leden van de CDA-fractie zich af of de huidige en voorziene bepalingen in het Wetboek van Strafvordering, totstandgekomen na een opeenstapeling van wetswijzigingen, nog wel voldoende overzichtelijk en hanteerbaar zijn. Voorop wil ik stellen dat de bedoelde wijzigingen, veelal aanvullingen van het Wetboek, steeds nauw aansluiten bij de feitelijke ontwikkelingen in de samenleving en bij de behoefte die juist ten gevolge dáárvan ontstaat aan nieuwe opsporingsbevoegdheden. Steeds heeft de wetgever daarbij gestreefd naar een zodanige inpassing in bestaande kaders dat de wet voor degenen die deze moeten toepassen, overzichtelijk en hanteerbaar blijft. Bovendien wordt onder verantwoordelijkheid van het openbaar ministerie, teneinde de toepassing te faciliteren, het Handboek voor de opsporing uitgegeven, waarin steeds ook de nieuwe bevoegdheden worden toegelicht en waarbij steeds ook het verband met bestaande bevoegdheden wordt aangegeven. Ik ben dan ook van mening dat de bevoegdheden nog voldoende overzichtelijk en hanteerbaar zijn. Dat neemt niet weg dat ik van mening ben, mede gelet op de vele wijzigingen van het wetboek die hebben plaatsgevonden, dat er reden is voor een herziening van het Wetboek van Strafvordering, niet beperkt tot het onderhavige terrein maar in veel breder verband. Ik verwijs daartoe graag naar mijn beleidsvoornemens op dit punt, neergelegd in mijn brieven over het «Algemeen kader herziening Wetboek van Strafvordering» (Kamerstukken II 2003/04, 29 271, nr. 1, en verder).

De leden van de D66-fractie vroegen of er bij politie, openbaar ministerie en rechterlijke macht voldoende kennis en menskracht aanwezig is voor een effectieve handhaving. Zoals ik hierboven al aangaf is het juist op een terrein als computercriminaliteit noodzakelijk om steeds te blijven investeren in het op peil brengen en houden van de kennis en vaardigheden die nodig zijn voor de opsporing en vervolging. Zowel bij de politie als bij het openbaar ministerie en de rechterlijke macht wordt op dit moment ook daadwerkelijk geïnvesteerd in het op peil brengen en houden van de benodigde kennis en vaardigheden. Dit is een continu proces omdat ontwikkelingen in de ICT-techniek – en daarmee in de bestrijding van computercriminaliteit – steeds voortschrijden. De verbreding en verdieping van kennis, zoals die bij de politie, het openbaar ministerie en de rechterlijke macht is ingezet, zal op termijn leiden tot een effectievere handhaving.

Artikelsgewijs

Artikelen 139d, tweede en derde lid, en 161sexies Sr.

De leden van de CDA-fractie hebben aandacht gevraagd voor de strafbaarstelling van voorbereidingshandelingen, zoals vormgegeven in de artikelen 139d, tweede en derde lid, en 161sexies, tweede lid, en hebben mijn mening gevraagd over de bewijsproblemen die deze bepalingen met zich mee kunnen brengen. Zij vroegen daarbij in het bijzonder aandacht voor het verband tussen «het oogmerk» en de elementen «technisch hulpmiddel» en «hoofdzakelijk geschikt gemaakt».
De leden van de fracties van VVD en PvdA achtten het voorgestelde artikel 139d, tweede lid, een zinvolle bepaling maar hadden twijfels over het derde lid van dat artikel in verband met de lastige bewijspositie waarin het openbaar ministerie daarbij komt te verkeren.

Aangezien de voorgestelde bepalingen nauw aansluiten bij artikel 6 van het Cybercrime Verdrag, wil ik om te beginnen nog eens de achtergrond van die verdragsbepaling aanstippen. Met name in de internetomgeving worden vaak middelen ter beschikking gesteld die gebruikt kunnen worden voor het begaan van strafbare feiten als omschreven in de artikelen 2 tot en met 5 van het Verdrag. Deze middelen zijn bijvoorbeeld

zogenaamde kraakprogramma's, *passwords* en toegangscodes waarmee onbevoegden toegang tot een computersysteem kunnen verkrijgen, maar het kan ook gaan om programma's die schade veroorzaken, zoals virussen en *worms*. Deze middelen kunnen ook bestaan in de vorm van apparaten of toestellen. In de opvatting van de verdragspartijen zou het in strafrechtelijke zin ongemoeid laten van het aanbod van dergelijke middelen ernstige risico's met zich brengen voor de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde gegevensbewerking en gegevens. Artikel 6 van het Verdrag richt zich dan ook tegen het vervaardigen, verspreiden of anderszins ter beschikking stellen van dergelijke middelen. Onder dit laatste wordt mede begrepen het opnemen van een zgn. hyperlink naar de site van waaraf deze middelen kunnen worden gedownload. Als delictshandelingen worden genoemd het vervaardigen, verkopen, verkrijgen voor gebruik, invoeren, verspreiden of anderszins beschikbaar stellen. Het enkele bezit van dergelijke middelen – daaronder mede te verstaan het ter beschikking stellen van deze middelen – is eveneens strafbaar. Voorwerp van het strafrechtelijk verbod zijn die middelen die *hoofdzakelijk* zijn ontworpen of beschikt gemaakt voor het begaan van de genoemde delicten. Uit de inrichting en de eigenschappen van het middel dient te blijken dat dit door de producent ook bedoeld is om een delict als omschreven in de artikelen 2 tot en met 5 van het Verdrag te begaan. Een cruciaal element in de strafbepaling is vervolgens dat het vervaardigen (etc.) geschiedt met het oogmerk dat het middel wordt gebruikt voor het plegen van (kort gezegd) computercriminaliteit. Anders dan de leden van de CDA-fractie menen, is er in de delictsomschrijving geen rechtstreeks verband tussen het «oogmerk» en het element dat het technisch hulpmiddel «hoofdzakelijk geschikt gemaakt of ontworpen» is voor een bepaald doel. Het *oogmerk* (van degene die de strafbare voorbereidingshandeling verricht) dient erop gericht te zijn dat met het technisch hulpmiddel (etc.) een misdrijf wordt gepleegd als bedoeld in artikel 138a, eerste lid, 138b of 139c, terwijl het technisch hulpmiddel (etc.) als zodanig in objectieve termen moet kunnen worden aangemerkt als «hoofdzakelijk geschikt gemaakt of ontworpen» tot het plegen van een zodanig misdrijf. Wel zullen in bepaalde omstandigheden de verschillende elementen feitelijk kunnen samenvallen, bijvoorbeeld als het gaat om de oorspronkelijke producent van het desbetreffende middel. Degene die een computerprogramma vervaardigt dat «hoofdzakelijk geschikt gemaakt of ontworpen» is tot het plegen van bijvoorbeeld computervredebreuk, is strafbaar wegens overtreding van artikel 139d, tweede lid, indien dat *vervaardigen* geschiedt met het oogmerk dat met dat computerprogramma ook daadwerkelijk computervredebreuk zal worden gepleegd. Degene die zo'n computerprogramma koopt of verkoopt, is strafbaar indien die *koop of verkoop* plaatsvindt met het oogmerk dat met dat computerprogramma ook daadwerkelijk computervredebreuk zal worden gepleegd.

Wat betreft de term «hoofdzakelijk» wijs ik erop dat in het Verdrag voor die term is gekozen en niet voor de term «uitsluitend» of «specifiek», omdat juist door die termen onoverkomelijke bewijsproblemen zouden ontstaan. De verdachte zou, om in een dergelijk geval vrijuit te gaan, slechts behoeven aan te tonen dat het middel ook voor enig ander gebruik geschikt is. De term «hoofdzakelijk» sluit niet uit dat ander, al dan niet legitiem, gebruik mogelijk is, maar impliceert dat zodanig ander gebruik als ondergeschikt moet worden beschouwd ten aanzien van de gebruiksmogelijkheden als hulpmiddel tot het begaan van een der in de artikelen 2 tot en met 5 van het Verdrag genoemde delicten (zie paragraaf 73 van het *Explanatory Memorandum*). Weliswaar had in het Cybercrime Verdrag ervoor gekozen kunnen worden om de bewijspositie sterk te vergemakkelijken door het schrappen van het element «hoofdzakelijk», maar de

verdragssluitende partijen hebben gemeend dat daarmee de strafbepaling een onaanvaardbaar grote reikwijdte zou krijgen.

De leden van de fracties van VVD en PvdA merkten op dat het in de praktijk al lastig zal zijn om vast te stellen dat iemand bijvoorbeeld over een wachtwoord beschikt met het oogmerk om computervredebreuk te gaan plegen (artikel 139d, tweede lid) en vroegen zich af hoe het dan ooit aan te tonen zou zijn dat iemand over een wachtwoord zou beschikken met het oogmerk (naaste doel) om gekwalificeerde computervredebreuk te gaan plegen (artikel 139d, derde lid); uit het enkele voorhanden hebben valt dit immers niet af te leiden, zo stellen deze leden. Het is zeker juist dat bepaalde feitencomplexen op dit terrein lastig te bewijzen zullen zijn, maar die omstandigheid laat naar mijn oordeel onverlet dat de wetgever die feitencomplexen op zichzelf genomen strafwaardig kan achten en derhalve strafbaar wil stellen. Daar komt bij dat er wel degelijk gevallen denkbaar zijn waarin het bewijs op het oogmerk van gekwalificeerde computervredebreuk goed te leveren zal zijn. Hiervoor kwam al aan de orde de situatie waarin iemand een computerprogramma vervaardigt of verkoopt (hiervoor aangeduid als een kraakprogramma), dat ontworpen is om computervredebreuk te plegen. Als dat computerprogramma dan tevens ontworpen is om de daardoor toegankelijk gemaakte gevens over te nemen en vast te leggen, is het voor artikel 139d, tweede lid, bedoelde bewijs in beginsel te leveren.

De leden van de fracties van VVD en PvdA hebben mij gevraagd nog eens aan te geven waarom in artikel 139d, derde lid, Sr de strafmaat voor de voorbereidingshandeling even hoog is gesteld als die voor het feit zelf dat wordt voorbereid, terwijl bij de strafbaarstelling van voorbereidingshandelingen in artikel 46 Sr bijvoorbeeld is gekozen voor de helft van de straf van het gronddelict. Ik heb daarvoor gekozen omdat het in artikel 139d steeds gaat om voorbereidingshandelingen die worden gepleegd met het «oogmerk» dat – eventueel door een ander – de grondfeiten worden gepleegd. Hierboven gaf ik al aan dat het soms inderdaad lastig kan zijn om het bewijs rond te krijgen dat iemand het oogmerk had dat een bepaald feit gepleegd zou worden. Maar áls dat bewijs dan geleverd kan worden, ligt het bij delicten als waarover het hier gaat voor de hand om voor de strafmaat aan te sluiten bij het feit waarop het oogmerk was gericht. Ik acht namelijk in algemene zin het daadwerkelijk plegen van computervredebreuk (artikel 138a Sr) niet verwerpelijker dan bijvoorbeeld het vervaardigen van een computerprogramma dat gericht is op het plegen van computervredebreuk, indien de vervaardiger ook het oogmerk heeft dat met dat hulpmiddel daadwerkelijk computervredebreuk wórdt gepleegd (artikel 139d, tweede lid). En als het computerprogramma dan ook nog gericht is op het plegen van een gekwalificeerde vorm van computervredebreuk (artikel 138a, tweede of derde lid) en het oogmerk van de maker dáárop gericht is, acht ik het wenselijk dat ook in dat geval wat betreft de strafmaat geen onderscheid wordt gemaakt tussen degene die uiteindelijk het grondfeit pleegt (en die dat misschien alleen kón doen dankzij het bestaan van het computerprogramma) en degene die, in de beperkte betekenis van artikel 139d, tweede of derde lid, daartoe een voorbereidingshandeling pleegde en het oogmerk had dat het feit ook gepleegd werd. In dat opzicht bestaat een verschil met de strafbaarstelling van voorbereidingshandelingen in artikel 46 Sr. Ten eerste is bij de daar bedoelde voorbereidingshandelingen geen oogmerk op het grondfeit vereist maar slechts opzet, waardoor ook voorwaardelijk opzet voldoende kan zijn. En ten tweede is artikel 46 Sr een algemene bepaling die geen verband legt met een of meer specifiek aangewezen strafbare feiten, wat in artikel 139d, tweede en derde lid, wel het geval is.

Artikel 125n Sv

De leden van de fracties van VVD en PvdA hebben gevraagd waarom er met betrekking tot de gegevens die bij onderzoek uit computersystemen worden vastgelegd, een wezenlijk ander regime wordt gekozen dan met betrekking tot gegevens die bijvoorbeeld door observatie of taps zijn verkregen. Dit verschil in regime bestaat reeds nu: het bestaande artikel 125n Sv kent immers, voor de eerstbedoelde categorie gegevens, als hoofdregel dat de gegevens worden vernietigd zodra ze van geen betekenis meer zijn, terwijl artikel 126cc voor de bijzondere categorie van gegevens die zijn verkregen met gebruikmaking van bepaalde bijzondere opsporingsbevoegdheden, uitgaat van een systeem waarin de gegevens pas worden vernietigd twee maanden nadat «de zaak is geëindigd». In het wetsvoorstel Computercriminaliteit-II was er aanvankelijk voor gekozen om ook voor de gegevens die vrijkomen bij een onderzoek in computersystemen, aan te sluiten bij het regime van artikel 126cc. Daarmee zouden echter in een aanmerkelijk groter aantal situaties dan thans het geval is, gegevens moeten worden bewaard, wat zowel uit een oogpunt van bescherming van de persoonlijke levenssfeer als uit een oogpunt van administratieve lasten niet zonder meer voor de hand lag. Het vraagstuk inzake het bewaren en vernietigen van gegevens die ter beschikking komen in het kader van het vooronderzoek, zal worden bezien in het hiervoor aangehaalde «Algemeen kader herziening Wetboek van Strafvordering». Zoals ik heb aangegeven in mijn brief van 9 november 2005 (Kamerstukken II 2005/06, 29 271, nr. 3, blz. 3), zullen in dat kader immers ook de bestaande bepalingen met betrekking tot dwangmiddelen, onderzoeksbevoegdheden en onderzoekshandelingen moeten worden doorgelicht en voor een deel opnieuw geformuleerd met inachtneming van de nieuwe structuur. Om deze reden worden vooralsnog geen wijzigingen aangebracht in de op het onderhavige terrein bestaande verschillen tussen artikel 125n en artikel 126cc Sv.

Artikel 125o Sv

Het verheugt mij dat de aan het woord zijnde leden het voorgestelde artikel 125o Sv, dat ziet op het ontoegankelijk maken van gegevens met een verboden karakter, een nuttige bepaling achten, die aansluit bij de problemen die zich in de praktijk op dit punt voordoen. Zij vroegen zich wel af of het systeem geheel sluitend is, omdat een zelfstandige bevoegdheid van de zittingsrechter ontbreekt om gegevens ontoegankelijk te maken en te vernietigen. Dit probleem, zo stelden deze leden, doet zich voor indien de officier van justitie of de rechter-commissaris niet al eerder gebruik heeft gemaakt van de bevoegdheid van artikel 125o Sv om gegevens ontoegankelijk te maken, bijvoorbeeld omdat de noodzaak daartoe ontbrak doordat het hele computersysteem (inclusief de verboden gegevens) in beslag was genomen. Inderdaad kan het voorkomen dat gegevens niet eerder ontoegankelijk zijn gemaakt omdat de gegevensdrager in beslag is genomen. Mocht de zittingsrechter oordelen dat het géén gegevens betreft met behulp waarvan of met betrekking waartoe het strafbare feit is gepleegd, dan wordt de gegevensdrager mét alle gegevens in beginsel weer teruggegeven. Als de zittingsrechter evenwel van oordeel is dat het wel gegevens betreft met behulp waarvan of met betrekking waartoe het strafbare feit is gepleegd, dan kan hij beslissen, de gegevensdrager te onttrekken aan het verkeer. Een gegevensdrager kan wel van de strafbare gegevens worden ontdaan zodat deze zónder de strafbare gegevens kan worden teruggegeven, maar om er zeker van te zijn dat alle strafbare gegevens daadwerkelijk zijn verwijderd, moet de gegevensdrager grondig worden gecontroleerd. Dit kost veel capaciteit van de betrokken opsporingsambtenaren. Om die reden wordt bijvoorbeeld in de Aanwijzing kinderpornografie voorgeschreven dat in een dergelijk geval

onttrekking aan het verkeer van de harde schijf wordt gevorderd. Als inbeslagneming van de gegevensdrager proportioneel was dan zal onttrekking aan het verkeer niet snel disproportioneel zijn, indien de rechter heeft vastgesteld dat er inderdaad strafbaar materiaal op staat. Ik meen dan ook dat de praktijk voldoende uit de voeten kan met de bestaande bevoegdheden en dat er geen behoefte is aan een specifieke bevoegdheid voor de zittingsrechter.

Inwerkingtreding artikel 273d, tweede lid, Sr

De leden van de CDA-fractie hebben gevraagd of de latere inwerkingtreding van artikel 273d, tweede lid, Sr niet zal leiden tot verwarring bij justitiabelen; de eerder aangegeven reden om een enkele bepaling uit het hele pakket van nieuwe strafbaarstellingen en bevoegdheden te halen, leek hen niet op voorhand overtuigend. Graag zet ik de achtergrond hiervan nog eens uiteen. De voorgestelde artikelen 273a tot en met 273e – met uitzondering van artikel 273d, tweede lid – zijn inhoudelijk niet nieuw maar zijn nagenoeg letterlijk gelijkluidend aan de huidige artikelen 372 tot en met 375, die nu nog in een andere titel van het Wetboek van Strafvordering zijn opgenomen. Voor de achtergrond van deze «verplaatsing» verwijs ik naar de uiteenzetting van mijn ambtsvoorganger in de memorie van toelichting op onderdeel L van artikel I van het wetsvoorstel (Kamerstukken TK 1998/99, 26 671, nr. 3, blz. 38, 39, 46 en 47). Inhoudelijk verandert er voor betrokkenen dus niets. Artikel 273d, eerste lid, is bijvoorbeeld gelijkluidend aan het huidige artikel 374bis en stelt kort gezegd strafbaar degene die, werkzaam bij een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, opzettelijk en wederrechtelijk een door tussenkomst van deze infrastructuur verzorgde, niet voor hem of niet mede voor hem bestemde gegevensoverdracht afluistert, aftapt of opneemt. Het tweede lid van artikel 273d is wél nieuw: het verruimt de reikwijdte van artikel 273d (het huidige 374bis) naar de niet-openbare telecommunicatienetwerken en -diensten. Onder welke omstandigheden sprake zal zijn van wederrechtelijk handelen van de rechthebbende – veelal de werkgever – en in welke gevallen de gegevens al of niet mede bestemd moeten worden geacht voor die rechthebbende, zal afhangen van de feitelijke beoordeling van de situatie, waarbij een grote betekenis zal moeten worden toegekend aan de afspraken die over het gebruik van de diensten en netwerken wordt gemaakt (zie ook Kamerstukken TK 2004/05, 26 671, nr. 7, blz. 18, 19, 37 en 38). Het komt mij wenselijk voor het bedrijfsleven voldoende tijd te gunnen voor het voorbereiden en maken van dergelijke afspraken, aangezien het hier een nieuwe strafbepaling betreft. Ik ben voornemens om, zodra het wetsvoorstel kracht van wet heeft verkregen, het bedrijfsleven op de hoogte te stellen van de nieuwe wetsbepaling en daarbij aan te kondigen op welke termijn deze in werking zal treden, waarbij ik voorshands denk aan een termijn van een half tot één jaar na plaatsing in het Staatsblad.

Toekomstige ontwikkelingen

Mét de leden van de VVD-fractie ben ik van mening dat het Cybercrime Verdrag en het wetsvoorstel Computercriminaliteit II een belangrijke stap in de richting van internationale samenwerking ter bestrijding van strafbare feiten verbonden met elektronische netwerken vormen, maar geen «finale oplossing» zijn. De ontwikkelingen staan inderdaad niet stil en natuurlijk zal op enig moment de wetgeving weer verder aangevuld moeten worden. Zeker valt ook niet uit te sluiten dat het op termijn wenselijk is om te komen tot een grotere mate van harmonisatie van strafbepalingen op het gebied van computercriminaliteit. Maar mijn eerste prioriteit is nu toch, ervoor te zorgen dat de nieuwe – nationale en internationale – instrumenten die met de inwerkingtreding van de onderhavige

wetsvoorstellen ter beschikking komen van de met opsporing en vervolging belaste instanties, ook daadwerkelijk ingezet gaan worden bij de bestrijding van computercriminaliteit.

Tenslotte

De leden van de CDA-fractie vroegen zich af of tijdens de behandeling van het wetsvoorstel de brief van het VNO/NCW van 21 juni 2005 aan de orde is geweest. Dat is niet het geval. De bedoelde brief was niet aan mij of aan de vaste commmissie voor Justitie van de Tweede Kamer gericht, maar aan de vaste commissie voor Verkeer en Waterstaat; tijdens de openbare behandeling van het wetsvoorstel is de brief bovendien door geen der sprekers aan de orde gesteld, noch zijn er vragen gesteld naar aanleiding van die brief. De leden van de CDA-fractie vragen mij thans naar aanleiding van het in die brief gestelde, in te gaan op de in het wetsvoorstel geïntroduceerde bevoegdheid tot het opnemen van communicatie zonder medewerking van een aanbieder.
Inmiddels heb ik kennis kunnen nemen van de inhoud van de brief. Ik begrijp dat het VNO/NCW het onwenselijk acht dat in besloten netwerken, zonder aankondiging vooraf, onderzoek zou kunnen worden verricht. Laat ik voorop stellen dat het nú op basis van artikel 126*l* Sv al mogelijk is om in besloten netwerken, zonder aankondiging vooraf, vertrouwelijke communicatie op te nemen met een technisch hulpmiddel. Daarbij kan het bijvoorbeeld gaan om het plaatsen van een *bug* in een computer voor het registreren van toetsaanslagen en muisklikken. Daarnaast is het op grond van het huidige artikel 125j óók al mogelijk – in het kader van een lopende doorzoeking – om vanaf de plaats waar die doorzoeking plaatsvindt, in een elders aanwezig geautomatiseerd werk onderzoek te doen naar gegevens die redelijkerwijs nodig zijn om de waarheid aan het licht te brengen, voor zover het althans gegevens betreft waartoe degene bij wie de doorzoeking plaatsvindt rechtmatig toegang heeft (denk aan de werknemer bij wie een doorzoeking plaatsvindt en die toegang heeft tot gegevensbestanden van de werkgever).
Tot zover is er dus niets nieuws onder de zon. Het onderhavige wetsvoorstel wijzigt echter het systeem van artikel 126m Sv, dat betrekking heeft op het *opnemen van telecommunicatie* met een technisch hulpmiddel. De werking van artikel 126m Sv wordt ter implementatie van het Cybercrime Verdrag in twee opzichten verruimd.

1. Ten eerste wordt de werking van het artikel niet meer beperkt tot het opnemen van communicatie die plaatsvindt door tussenkomst van een aanbieder van openbare telecommunicatie maar uitgebreid tot communicatie die plaatsvindt door middel van de diensten van een aanbieder van een communicatiedienst, waaronder ook private netwerken vallen.
2. Ten tweede wordt voor bijzondere gevallen de mogelijkheid geïntroduceerd dat het opnemen plaatsvindt zonder de medewerking van de aanbieder.

Hoofdregel bij dit alles blijft natuurlijk dat de aanbieder wel degelijk in de gelegenheid wordt gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel van de officier van justitie; dat ligt uitdrukkelijk in de wettekst besloten en bovendien is het in de praktijk ook veel gemakkelijker om mét medewerking van de aanbieder communicatie op te nemen. Alleen als het belang van strafvordering zich daartegen verzet, kan van het vragen van medewerking worden afgezien.
Maar in dat geval gelden enkele bijzondere waarborgen (zie ook de toelichting op de tweede nota van wijziging, Kamerstukken TK 2004/05, 26 671, nr. 7, blz. 29). De rechter-commissaris dient expliciet toestemming te geven voor het bevel van de officier van justitie. Daarnaast wordt uitdrukkelijk bepaald dat, indien het opnemen geschiedt zonder medewerking van de aanbieder, het technisch hulpmiddel moet voldoen aan bij

algemene maatregel van bestuur te stellen eisen. De vrees van het VNO/NCW dat door opsporingsinstanties hetzelfde instrumentarium kan worden ingezet als door computercriminelen is in die zin dan ook ongegrond. De technische hulpmiddelen zullen moeten voldoen aan de bij algemene maatregel van bestuur te stellen eisen. En vanzelfsprekend wordt de algemene maatregel van bestuur ter consultatie voorgelegd aan de betrokken instanties, waaronder het VNO/NCW.

Ik hoop met het voorgaande de in het voorlopig verslag gestelde vragen naar tevredenheid te hebben beantwoord.

De Minister van Justitie,
J. P. H. Donner