Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

33 400 VI Vaststelling van de begrotingsstaten van het Ministerie van Veiligheid en Justitie (VI) voor het jaar 2013

Nr. 68 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 november 2012

Bij de bestrijding van kinderpornografie wordt de politie geconfronteerd met de effecten van het (toenemend) gebruik van encryptie/versleuteling van bestanden door computergebruikers. Dit is in het kader van de Rotterdamse proeftuin kinderpornografie aan de orde gekomen. Ook het opsporingsonderzoek in de Amsterdamse zedenzaak bleek dat de verdachte Robert M. grote hoeveelheden kinderpornografie in versleutelde vorm op zijn computer had opgeslagen. Tijdens het Algemeen Overleg over de aanpak van kinderpornografie, dat op 17 mei 2011 is gehouden, is door de CDA-fractie op dit probleem gewezen. De CDA-fractie zou graag zien dat het verplicht wordt dat verdachten meewerken aan het openen van die bestanden. Daarbij is gewezen op de regeling in Engeland, die het mogelijk maakt om een verdachte om de toegangscode te vragen (Kamerstukken 2010/11, 32 500 VI, nr. 107).

In mijn brief van 27 januari 2012 (Kamerstukken 2011/12, 31 015, nr. 77) heb ik Uw Kamer geïnformeerd over de ervaringen in het Verenigd Koninkrijk met het bevel tot het ontsleutelen van versleutelde gegevens (hierna ook te noemen: decryptiebevel). Naar aanleiding van de ervaringen in het Verenigd Koninkrijk heb ik melding gemaakt van mijn positieve houding ten opzichte van het bevorderen van een vergelijkbare regeling in de Nederlandse strafwetgeving. Dit vanwege het belang van een effectieve bestrijding van de vervaardiging, de verspreiding en het bezit van kinderpornografie. Daarbij is opgemerkt dat binnen het Nederlandse stelsel van strafvordering een verdachte niet kan worden verplicht mee te werken aan zijn eigen veroordeling.

Het Nederlandse Wetboek van Strafvordering voorziet in de mogelijkheid om, in geval van een doorzoeking ter vastlegging van gegevens, aan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de beveiliging van een geautomatiseerd werk, een bevel te richten toegang te verschaffen tot de aanwezige geautomatiseerde werken of

kst-33400-VI-68
ISSN 0921 - 7371
's-Gravenhage 2012

delen daarvan. Degene tot wie het bevel is gericht dient desgevraagd hieraan gevolg te geven door de kennis omtrent de beveiliging ter beschikking te stellen. Een soortgelijk bevel kan worden gegeven indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen. Het bevel richt zich tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens. Een dergelijk bevel kan echter niet aan de verdachte worden gericht (art. 125k Sv). Dit vanwege het beginsel van nemo tenetur.

Een verplichting voor een verdachte om gegevens te ontsleutelen is in de Europese Unie bepaald geen vanzelfsprekendheid. Voorzover thans bekend, kennen uitsluitend het Verenigd Koninkrijk en Frankrijk een dergelijke verplichting. De wettelijke regeling van deze landen is tot nu toe echter niet aan het Europese Hof voor de bescherming van de Rechten van de Mens en de fundamentele vrijheden (EHRM) voorgelegd. Alvorens tot het in voorbereiding nemen van wetgeving te besluiten, achtte ik dan ook nader onderzoek noodzakelijk naar de verenigbaarheid van een decryptiebevel aan verdachten met het in artikel 6 EVRM vervatte nemo-teneturbeginsel. Dit teneinde te voorkomen dat een eventuele Nederlandse wettelijke regeling in strijd zou zijn met artikel 6 van het EVRM.

Aan het Centrum voor Recht, Technologie en Veiligheid van de Universiteit van Tilburg is opdracht gegeven een nader onderzoek te verrichten. In 2000 heeft prof. dr. E.J. Koops, verbonden aan het Centrum voor Recht, Technologie en Veiligheid, reeds een omvangrijke studie gepubliceerd over het decryptiebevel aan de verdachte (Koops 2000). In die studie werd geconcludeerd dat, in het licht van de Nederlandse wetgeving, een ontsleutelplicht voor verdachten in het commune strafrecht een unieke bevoegdheid zou zijn en dat de wetgever daarom zeer zwaarwichtige redenen zou moeten hebben om een dergelijke bevoegdheid in te voeren. Tegen die achtergrond is in het nieuwe onderzoek als hoofdvraag onderzocht in hoeverre, gelet op de ontwikkelingen sinds 2000, een decryptiebevel verenigbaar is met het nemo-teneturbeginsel. Het nieuwe onderzoek is beperkt tot het commune strafrecht, waarbij één van de aandachtspunten was of een ontsleutelplicht specifiek dient te worden gericht op bepaalde delicten, zoals kinderporno, of generiek op alle typen (ernstige) strafbare feiten.

Inmiddels is het onderzoek van het Centrum voor Recht, Technologie en Veiligheid afgerond. Het rapport, getiteld «Decryptiebevel en artikel 6 EVRM», bied ik u hierbij aan (Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer). Het rapport is voorzien van een korte samenvatting (Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer), waarin de belangrijkste bevindingen zijn weergegeven. Ik heb met veel waardering kennisgenomen van de inhoud van het rapport. Het Centrum voor Recht, Technologie en Veiligheid heeft een gedegen rapport opgeleverd, dat een goed inzicht biedt in de verenigbaarheid van het nemo-teneturbeginsel met artikel 6 van het EVRM. Het rapport biedt dan ook een uitstekende basis voor de verdere beleids- en besluitvorming.

In het rapport wordt de jurisprudentie van het EHRM geanalyseerd en worden de ontwikkelingen in het Nederlandse recht beschreven. Het Nederlandse recht inzake nemo tenetur is sinds 2000 niet substantieel gewijzigd. De jurisprudentie van de Hoge Raad sluit aan bij de rechtspraak van het EHRM. Deze jurisprudentie steunt op het beginsel dat het gebruik van een verklaring in een strafzaak niet het zwijgrecht, en daarmee het recht zichzelf niet te belasten, van zijn betekenis mag ontdoen. In het rapport worden enkele ontwikkelingen beschreven rond het verbinden van consequenties aan de weigering van een verdachte om mee te

werken aan het opsporingsonderzoek. In de bekende Amsterdamse zedenzaak is de weigering te verklaren over wachtwoorden gebruikt bij de verwerping van een verweer. Ook kan het gebruik van het zwijgrecht leiden tot verhoging van de op te leggen straf of meewegen bij de beslissing over de onttrekking aan het verkeer van inbeslaggenomen gegevensdragers. Dit biedt de rechter de ruimte om de weigering van een verdachte om een harde schijf of versleutelde bestanden toegankelijk te maken in situaties waarin de aanwezigheid van de bestanden duidelijk vragen oproept, mee te laten wegen in het bewijs, de straftoemeting of andere beslissingen ten nadele van de verdachte.

In het rapport worden de wettelijke regelingen in enkele andere landen, zoals Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten, uitgebreid beschreven. In de Franse Code pénal is, met de zogenoemde Wet op de dagelijkse veiligheid, een afzonderlijke bepaling opgenomen op grond waarvan degene, die kennis heeft van een geheime decryptiesleutel van een cryptologisch middel dat gebruikt kan zijn om een misdrijf of overtreding voor te bereiden, te faciliteren of te plegen en die weigert de sleutel op vordering van de autoriteiten te overhandigen, gestraft kan worden met een gevangenisstraf van drie jaar en een boete van 45 000 euro (artikel 434-15-2). Als de weigering is geschied terwijl de overhandiging of toepassing van de sleutel het mogelijk gemaakt zou hebben een misdrijf te voorkomen of de effecten hiervan te verminderen, dan kan de straf worden verhoogd naar vijf jaar gevangenisstraf en een boete van 75 000 euro. Daarnaast vormt het gebruik van encryptie een grond voor verhoging van de maximumgevangenisstraf met één categorie. Het bevel kan ook aan de verdachte worden gegeven. Tot nu toe is geen jurisprudentie bekend over de toepassing van de decryptieverplichting of de verhouding met het in artikel 6 EVRM vastgelegde beginsel van nemo tenetur.
In het Verenigd Koninkrijk is, met de Regulation of Investigative Powers Act 2000 (RIPA), een omvangrijke en complexe regeling van het ontsleutelbevel ingevoerd. Een ambtenaar van politie, de veiligheidsdienst of de douane kan een persoon die redelijkerwijs geacht kan worden de sleutel te hebben, een schriftelijk bevel geven om de beschermde informatie vrij te geven in het belang van – onder meer – de voorkoming of ontdekking van strafbare feiten (s. 49 RIPA). De strafbedreiging is een gevangenisstraf van twee jaar, met een maximum van vijf jaar in terroristische zaken en kinderpornografie. Voor een ontsleutelbevel is rechterlijke toestemming nodig als de gegevens zijn verkregen op basis van een bevoegdheid die een rechterlijke machtiging vereist. In de andere gevallen is een opsporingsambtenaar zelf bevoegd een ontsleutelbevel te geven, wanneer zijn functie een bepaald niveau vertegenwoordigt («superintendent») of met toestemming van een opsporingsambtenaar van dat niveau. Vooraf dient het National Technical Assistance Centre (NTAC) te worden geconsulteerd over de uitoefening van de bevoegdheid. De aanvragen worden door het NTAC geregistreerd. Daarnaast oefenen de Chief Surveillance Commissioner en de Interception of Communications Commissioner onafhankelijk toezicht uit op de toepassing van de bevoegdheid. Door de toezichthoudende autoriteiten wordt ieder jaar een openbare rapportage opgesteld. Inmiddels heeft het Engelse Court of Appeal geoordeeld dat het ontsleutelbevel niet in strijd is met het in artikel 6 van het EVRM vastgelegde recht op een eerlijk proces. Daarbij is getoetst of de procedure in zijn geheel eerlijk is geweest. Indien het ontsleutelde materiaal inderdaad belastend blijkt te zijn, kan de rechter alsnog besluiten om dit materiaal uit te sluiten van het bewijs indien hij in een concreet geval oordeelt dat het nemo tenetur beginsel is geschonden.

In het rapport wordt opgemerkt dat de Britse regeling de meeste aanknopingspunten voor de Nederlandse beleidsvorming biedt. Daarbij

wordt erop gewezen dat de Britse regeling niet alleen zeer gedetailleerd is maar ook met veel waarborgen omkleed. Dit betreft de gevallen waarin ontsleuteling kan worden bevolen, de redelijke bewijslastverdeling als de verdachte betoogt niet in staat te zijn te ontsleutelen, het vereiste van rechterlijke toestemming, de schriftelijke vorm van het bevel en de controle door een speciale onafhankelijke autoriteit (de Chief Surveillance Commissioner of de Interception of Communications Commissioner). Omdat Nederland een dergelijke toezichthouder niet kent dient het algehele stelsel van checks and balances goed te worden bekeken als opsporingsbevoegdheden uit het Britse recht door Nederland worden overgenomen.

In het rapport wordt vastgesteld dat het gebruik van encryptie door verdachten toeneemt, in het bijzonder bij de opslag van gegevens en vooral bij bepaalde groepen kinderpornonetwerken. Dit wordt gefaciliteerd door software waarmee bestanden gemakkelijk versleuteld kunnen worden, zelfs op zodanige wijze dat het versleutelde bestand zelf niet kenbaar is. Op basis van de analyse van de Europese en Nederlandse jurisprudentie en de situatie in andere landen wordt geconcludeerd dat een decryptiebevel voor verdachten nog steeds zou afwijken van het systeem van de Nederlandse wetgeving, voor zover de weigering mee te werken strafbaar zou zijn. Onder bepaalde strenge voorwaarden is een ontsleutelplicht voor verdachten echter niet onverenigbaar met het nemo-teneturbeginsel. De regeling moet dan wel zeer zorgvuldig en afgewogen zijn en rekening houden met alle criteria die het EHRM aanlegt. De relevante factoren, die tezamen en in hun onderlinge samenhang dienen te worden afgewogen om te bepalen of de afgedwongen medewerking aanvaardbaar is in het licht van het nemo-teneturbeginsel, betreffen de aard en mate van de dwang (1), het gewicht van het publieke belang (2), de aanwezigheid van relevante waarborgen in de procedure (3) en de manier waarop het afgedwongen materiaal wordt gebruikt (4). Aangezien de situatie sinds 2000 veranderd is verdient het aanbeveling dat een hernieuwde afweging wordt gemaakt of en onder welke omstandigheden een decryptiebevel aan verdachten zou kunnen worden gegeven.

In het rapport worden verschillende opties voor een ontsleutelplicht onderzocht. De eerste optie (optie A) betreft een decryptieregeling conform de regeling van het verhoor in het Wetboek van Strafvordering. Dit betekent dat artikel 125k, derde lid, van het Wetboek van Strafvordering wordt gewijzigd zodat een bevel tot het ontsleutelen van gegevens aan een verdachte kan worden gegeven. Vanwege het zwijgrecht van de verdachte – dat in artikel 29 van het Wetboek van Strafvordering is vastgelegd – is een verdachte niet gehouden aan een dergelijk bevel medewerking te verlenen. Het bevel heeft materieel dus de betekenis van een formeel verzoek. Voor het verhoor dient de verdachte te worden medegedeeld dat hij niet tot antwoorden is verplicht (art. 29, tweede lid, Sv). De verdachte kan in volledige vrijheid zijn wil bepalen. Indien hij besluit niet mee te werken zal hij langer voorwerp van onderzoek kunnen zijn. Daar komt bij dat de rechter aan een eventuele weigering om medewerking te verlenen de consequenties kan verbinden die hij geraden acht. Zoals hiervoor aan de orde is gekomen mag de rechter een belastende omstandigheid, waarvoor de verdachte weigert een enigszins plausibele verklaring te geven, meewegen in de waardering van de bewijsmiddelen, de beoordeling van verweren, de straftoemeting of bij andere beslissingen ten nadele van de verdachte.

De tweede optie (optie B) betreft een decryptiebevel met bewijsuitsluiting. Hierbij kan onderscheid worden gemaakt tussen een verzoek en een bevel tot het ontsleutelen van gegevens. De mogelijkheid van een verzoek

vereist geen wettelijke regeling; de officier van justitie kan toezeggen de resultaten van de medewerking van de verdachte niet als bewijs tegen hem te zullen gebruiken. De bevoegdheid tot het geven van een bevel vereist echter een wettelijke regeling, conform optie A. Desgewenst kan de niet nakoming van een bevel strafbaar worden gesteld. Gemeenschappelijk kenmerk van deze beide varianten is dat er gering risico bestaat voor inbreuk op het beginsel van nemo tenetur, omdat er geen sprake is van zelfbelasting. De bewijsuitsluiting strekt zich uit over zowel de door de verdachte verstrekte gegevens als over het afgeleide bewijs. Een decryptiebevel met de strafbaarstelling van weigering kan van belang zijn in die gevallen waarin er een dringend belang is bij de hulpverlening aan slachtoffers, bijvoorbeeld omdat deze zich in gevaarlijke of mensonterende omstandigheden bevinden en het dringend noodzakelijk is dat het strafbaar handelen jegens hen onmiddellijk wordt beëindigd. Deze optie kan dan als laatste redmiddel dienen als het materiaal op geen enkele andere wijze kan worden achterhaald of in de gevallen waarin reeds voldoende bewijsmateriaal voorhanden is.

De derde optie (optie C) betreft een decryptiebevel met strafbaarstelling van weigering. Dit betekent dat aan de verdachte een bevel kan worden gegeven tot het ontsleutelen van gegevens. Als de verdachte medewerking weigert, kunnen aan een dergelijke weigering verschillende consequenties worden verbonden. De eerste mogelijkheid is een strafbaarstelling van weigering (optie C1). De tweede mogelijkheid is het verbinden van belastende gevolgtrekkingen aan weigering, bij de waardering van de bewijsmiddelen of bij de straftoemeting (optie C2). De derde mogelijkheid is de opneming van een expliciete strafverhogingsgrond voor het betreffende gronddelict in het Wetboek van Strafrecht (optie C3).

In het rapport wordt gewezen op mogelijke handhavingsproblemen rond een wettelijke verplichting van de verdachte tot het ontsleutelen van gegevens. Dit betreft de mogelijkheid om aan te tonen dat een verdachte in staat is te ontsleutelen. Tijdens het opsporingsonderzoek kan blijken van aanwijzingen dat een verdachte beschikt over afgeschermde en versleutelde gegevensbestanden. Het is uiteindelijk aan de rechter om hierover te beslissen maar er kunnen zich dan situaties voordoen waarin van een verdachte kan worden gevraagd om nadere uitleg omtrent de beschikbaarheid en de inhoud van de bestanden. Vanwege de ontwikkelingen op het gebied van de jurisprudentie worden deze problemen in vergelijking met de eerdere studie uit 2000 minder zwaarwegend ingeschat.

In het rapport wordt opgemerkt dat, vanuit het oogpunt van het systeem van de wet, in ieder geval serieus de mogelijkheid van een decryptieregeling conform de regeling van het verhoor overwogen zou moeten worden (optie A). De keuze tussen de twee andere opties komt vooral neer op een beleidsafweging. In het rapport wordt een aantal overwegingen geformuleerd ten aanzien waarvan het aanbeveling verdient die bij de beleidsafweging te betrekken. Deze overwegingen hebben betrekking op de effectiviteit van een ontsleutelplicht. Hiervan mogen geen wonderen worden verwacht vanwege de technische ontwikkeling van software die de toepassing van encryptie verbetert en vereenvoudigt en het risico dat berekenende criminelen niet zullen meewerken aan het ontsleutelen van gegevens. Ook wordt gewezen op alternatieve mogelijkheden, zoals het op afstand heimelijk binnendringen en doorzoeken van geautomatiseerde werken teneinde wachtwoorden of sleutels te achterhalen.

In reactie op de bevindingen van het rapport merk ik op dat ik veel waarde hecht aan de bestrijding van vormen van criminaliteit, zoals het bezit en

de handel in kinderpornografie, waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van de encryptie van elektronische gegevens. Voor een adequate bestrijding van deze strafbare feiten is het van groot belang dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens. Het is in het belang van het opsporingsonderzoek dat de strafbare feiten worden beëindigd door de aanhouding van de daders. Dit is ook in het belang van de veelal minderjarige slachtoffers. Met behulp van de beelden kan het openbaar ministerie in contact komen met de ouders of verzorgers van de slachtoffers en informatie en voorlichting verschaffen over de gepleegde strafbare feiten en over de mogelijkheden op het gebied van hulpverlening.

De decryptieregeling conform het verhoor (optie A) sluit goed aan bij de regeling van het verhoor van de verdachte in het Wetboek van Strafvordering. Er is ook nauwelijks sprake van een reeël risico van strijdigheid met het beginsel van nemo tenetur omdat er materieel sprake is van een verzoek tot medewerking aan de verdachte. Aan een weigering tot medewerking kan een rechter consequenties verbinden ten nadele van de verdachte. Naar mijn oordeel is een zwaarwegend bezwaar van deze optie dat de medewerking van de verdachte niet afdwingbaar is. Dit zal de effectiviteit van de regeling ernstig kunnen aantasten. Een ontsleutelverzoek zal waarschijnlijk niet werken bij berekenende criminelen, die geen medewerking willen verlenen. Juist bij verdachten van het bezit en de handel in kinderpornografie zal dit aan de orde kunnen zijn.

Het decryptiebevel met bewijsuitsluiting (optie B) leidt niet tot een inbreuk op het nemo-teneturbeginsel omdat een verdachte niet wordt gedwongen zichzelf te belasten. De meerwaarde kan zijn gelegen in het verzamelen van bewijsmateriaal tegen anderen of in het achterhalen van slachtoffers zodat aan hen hulp kan worden verleend. Dit vergt echter, zoals in het rapport ook wordt opgemerkt, een afweging tussen het belang van vervolging van de verdachte en het belang van het slachtoffer. Strikt genomen behoeft een verzoek waarbij de verdachte op vrijwillige basis om medewerking wordt gevraagd geen wettelijke regeling. Dit ligt anders bij een bevel tot medewerking. Om het bevel afdwingbaar te doen zijn is strafbaarstelling van de niet-nakoming vereist. Dan dient zich eenzelfde afweging aan als bij een decryptiebevel met strafbaarstelling, namelijk de aard en hoogte van de strafbedreiging. Bovendien wordt dan bewijsmateriaal, dat rechtmatig is verkregen, bij voorbaat uitgesloten van het bewijs. Een dergelijk systeem, waarbij een verdachte immuniteit voor strafvervolging verkrijgt door medewerking te verlenen aan het opsporingsonderzoek, past niet goed in het Nederlandse stelsel van strafvordering.

Het decryptiebevel met de strafbaarstelling van weigering (optie C) kan op twee verschillende manieren worden gerealiseerd. In de eerste plaats kan artikel 125k, derde lid, van het Wetboek van Strafvordering worden geschrapt, waardoor een decryptiebevel ook tot de verdachte kan worden gericht. Indien de verdachte medewerking weigert maakt hij zich schuldig aan het niet opvolgen van een bevoegd gegeven ambtelijk bevel (art. 184 Sr), waarop een gevangenisstraf van ten hoogste drie maanden is gesteld. Gelet op de ernst van de gedragingen die hierbij aan de orde zijn, het georganiseerde karakter van het strafbaar handelen en de strafbedreiging op het hoofddelict, acht ik een dergelijke strafbedreiging niet voldoende afschrikwekkend. Dit zal ernstig afbreuk doen aan de effectiviteit van de regeling bij de verdenking van ernstige strafbare feiten waarbij de daders zich hebben toegelegd op het versleutelen van belastende informatie. Het alternatief is een zelfstandige strafbaarstelling van het, in geval van verdenking van bepaalde ernstige strafbare feiten, opzettelijk niet voldoen aan een bevoegd gegeven bevel tot het toegankelijk maken van versleu-

telde gegevens. De strafbedreiging dient in evenwicht te zijn met de aard van het onderliggende strafbare feit enerzijds en met de uit artikel 6 EVRM voortvloeiende vereisten anderzijds. Te dien aanzien wordt er in het rapport op gewezen dat een hogere straf effectiever zal zijn, maar eerder in strijd zal kunnen komen met de vereisten van het EVRM.

Op basis van de afweging van de verschillende opties gaat mijn voorkeur uit naar opneming in het Wetboek van Strafvordering van een bevoegdheid tot het geven van een bevel aan een verdachte tot het verschaffen van toegang tot versleutelde elektronische gegevens en het toegankelijk maken van die gegevens. Een persoon die de nodige inspanningen heeft verricht om zijn strafbare gedragingen te verhullen moet rekening met de inzet van zwaardere middelen om de waarheid aan de dag te brengen. Dit neemt niet weg dat dit een zeer verstrekkende bevoegdheid betreft. Mede in het licht van de eisen van artikel 6 EVRM wordt de uitoefening beperkt tot de vervaardiging, de verspreiding en het bezit van kinderpornografie (art. 240b Sr) en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens. Het publieke belang van de bestrijding van dergelijke vormen van criminaliteit waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van de encryptie van elektronische gegevens noopt tot een specifieke bevoegdheid tot het toegankelijk maken van dergelijke gegevens. Het bevel kan zowel de beschikbaarstelling van gegevens ten behoeve van de toegang tot een geautomatiseerd werk als tot versleutelde elektronische gegevens omvatten. Daarbij zullen zeer strikte waarborgen moeten gelden voor de uitoefening en toepassing van deze bevoegdheid. Een bevel kan uitsluitend worden gegeven als het belang van het opsporingsonderzoek dat dringend vordert. Het bevel zal uitsluitend gegeven kunnen worden door de officier van justitie, na schriftelijke machtiging van de rechter-commissaris. Daardoor is rechterlijke controle gewaarborgd voordat de bevoegdheid wordt ingezet. Bij de beoordeling van het dringende belang van het opsporingsonderzoek zal de rechter-commissaris toetsen of aan de wettelijke voorwaarden en de ongeschreven beginselen van een behoorlijke procesorde, zoals de beginselen van proportionaliteit en subsidiariteit, is voldaan. Het bevel dient uitsluitend schriftelijk te worden gegeven. Tenslotte zal worden voorzien in een evaluatie en een horizonbepaling.

Vanwege de ernst van de betreffende strafbare feiten ligt het in de rede dat het opzettelijk niet voldoen aan het bevel tot het toegankelijk maken van gegevens afzonderlijk strafbaar wordt gesteld. Hierbij moet worden opgemerkt dat het strafbare karakter van de gedraging uitsluitend betrekking heeft op het weigeren medewerking te verlenen aan een bevel van een bevoegde ambtenaar tot het verstrekken van informatie. Het ernstige strafbare feit, ten aanzien waarvan de verdenking bestaat, is niet bewezen. Tot nu toe ligt de strafbedreiging voor het opzettelijk weigeren van medewerking aan een bevel of een vordering of het niet nakomen van een verplichting aanzienlijk lager. Het opzettelijk niet voldoen aan een bevoegd gegeven ambtelijk bevel is, zoals hierboven reeds is gemeld, strafbaar gesteld met een gevangenisstraf van ten hoogste drie maanden (art. 184 Sr). De getuige die opzettelijk niet voldoet aan zijn verplichting te verklaren, kan worden gestraft met een gevangenisstraf van ten hoogste een jaar (art. 192, tweede lid, Sr). De strafbedreiging zal moeten worden beoordeeld in relatie tot alle factoren die van invloed zijn op de beoordeling van een mogelijke schending van het EVRM. Dit betreft de aard en ernst van het strafbaar feit (publieke belang), de hoogte van de strafbedreiging (mate van dwang) en de strafprocessuele waarborgen voor de verdachte. Gelet op deze factoren acht ik een strafbedreiging, die substantieel hoger is dan de strafbedreiging voor het niet opvolgen van

een bevoegd gegeven ambtelijk bevel, gerechtvaardigd. De keuze voor een specifieke strafbedreiging zal in het wetsvoorstel nader worden beargumenteerd.

Ik ben mij bewust van de risico's op het gebied van de handhaving van een decryptiebevel. Het is niet ondenkbaar dat een wettelijke verplichting tot het toegankelijk maken van elektronische gegevens leidt tot een verdere ontwikkeling van software waarmee gegevensbestanden aan het zicht van buitenstaanders kunnen worden onttrokken. Naar mijn oordeel kan dit echter geen doorslaggevende reden zijn om af te zien van aanpassing van het wettelijk instrumentarium op dit gebied. De ontwikkelingen op het gebied van de informatietechnologie gaan steeds verder, waardoor de rechtshandhaving op grotere achterstand komt. Met een wettelijke regeling van een decryptiebevel wordt het juridisch instrumentarium van politie en justitie om toegang kunnen verkrijgen tot versleutelde gegevens aangepast aan de eisen van deze tijd. Een dergelijke bevoegdheid kan meerwaarde hebben als onderdeel van het pakket aan bevoegdheden van politie en justitie om de vervaardiging, de verspreiding en het bezit van kinderpornografie effectief te bestrijden. De ervaring in het Verenigd Koninkrijk wijst uit dat de dreiging van een decryptiebevel dikwijls afdoende is om een verdachte tot medewerking te bewegen. Niettemin wordt de inzet van de bevoegdheid in dat land enkele tientallen malen per jaar aangevraagd en tenuitvoergelegd. Een klein deel van de gevallen, waarin medewerking is geweigerd, heeft geleid tot vervolging en een veroordeling door de rechter. Zo blijkt uit het jaarverslag van de Chief Surveillance Commissioner dat in de periode 2011–2012 twintig bevelen zijn uitgevaardigd, waarbij in negen gevallen tot vervolging is over gegaan.

Voor wat betreft de procedurele waarborgen ligt oriëntatie op de regeling van het Verenigd Koninkrijk voor de hand. Daarbij moet worden benadrukt dat het Engelse rechtsstelsel op essentiële onderdelen afwijkt van het Nederlandse systeem. Dit betreft zowel de positie van de rechter als de procedures rond het bewijs. En anders dan het Verenigd Koninkrijk kent Nederland geen onafhankelijk toezichthoudend orgaan dat kan worden belast met het toezicht op de toepassing van de bevoegdheid in de praktijk. In plaats daarvan zal de rechter-commissaris kunnen toezien op de toepassing van de bevoegdheid. Dit past in het Nederlandse systeem van strafvordering waarbij de toepassing van ingrijpende opsporingsbevoegdheden, zoals het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie, afhankelijk is van een voorafgaande schriftelijke machtiging van de rechter-commissaris. Er zijn echter meer verschillen met de Britse regeling. In de eerste plaats zal de bevoegdheid tot het geven van een bevel tot het toegankelijk maken van gegevens worden beperkt tot bepaald aangewezen, ernstige strafbare feiten. In de tweede plaats zal de bevoegdheid uitsluitend uitgeoefend kunnen worden op basis van een bevel van de officier van justitie. De opsporingsambtenaar is daartoe niet zelfstandig bevoegd. Op deze punten is de Britse regeling ruimer.

Bij brief van 15 oktober 2012 heb ik Uw Kamer geïnformeerd over noodzakelijke, nieuwe strafrechtelijke opsporingsbevoegdheden op het internet (Kamerstukken II, 2012/13, 28 684, nr. 363). In die brief is aangegeven dat, mede in het licht van de technologische ontwikkelingen, een wettelijke bevoegdheid dient te worden gecreëerd om op afstand heimelijk een geautomatiseerd werk binnen te dringen ten behoeve van de opsporing van ernstige vormen van cybercrime. Hierboven is aangegeven dat er duidelijke raakvlakken zijn tussen een dergelijke bevoegdheid, die ook kan ook worden ingezet om beveiligingscodes of wachtwoorden van versleutelde gegevensbestanden te achterhalen, en de

bevoegdheid tot het geven van een decryptiebevel. Een conceptwetsvoorstel voor het op afstand heimelijk binnendringen van een geautomatiseerd werk is echter nog in voorbereiding. Bovendien zal het op afstand doorzoeken van een geautomatiseerd werk niet in alle gevallen leiden tot het achterhalen van gegevens die de mogelijkheid bieden om versleutelde gegevensbestanden te openen. De daarvoor benodigde gegevens kunnen eenvoudig op een afzonderlijke gegevensdrager worden opgeslagen. Daarom meen ik dat er aanleiding bestaat tot het creëren van een afzonderlijke wettelijke bevoegdheid tot het afgeven van een bevel of een vordering aan een verdachte dat hij versleutelde gegevens toegankelijk maakt. Er kan dan, afhankelijk van de specifieke omstandigheden van het geval, worden gekozen voor de inzet van één van deze bevoegdheden om te komen tot het gewenste resultaat, te weten de toegang tot de versleutelde gegevens ten behoeve van het opsporingsonderzoek naar kinderpornografie en terrorisme.

Op basis van de hierboven weergegeven kaders ben ik voornemens een wetsvoorstel voor te bereiden. Naar verwachting zal dit wetsvoorstel volgend voorjaar in consultatie kunnen worden gegeven.

De minister van Veiligheid en Justitie,
I. W. Opstelten