Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 1629

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 6 juni 2013

De vaste commissie voor Veiligheid en Justitie en de vaste commissie voor Europese Zaken hebben op 24 april 2013 overleg gevoerd met minister Opstelten van Veiligheid en Justitie over:

- **het voorstel van de Europese Commissie d.d. 4 april 2013 «Netwerk en informatiebeveiliging in de Unie COM (2013) 48» (2013Z06816);**
- **de brief van de minister van Buitenlandse Zaken d.d. 15 maart 2013 ter aanbieding van het fiche inzake Richtlijn netwerk- en informatiebeveiliging (Kamerstuk 22 112, nr. 1587).**

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Justitie,
Jadnanansing

De voorzitter van de vaste commissie voor Europese Zaken,
Knops

De griffier van de vaste commissie voor Justitie,
Nava

kst-22112-1629
ISSN 0921 - 7371
's-Gravenhage 2013

Voorzitter: Verhoeven
Griffier: Mittendorff

Aanwezig zijn vier leden der Kamer, te weten: Dijkhoff, Gesthuizen, Oosenbrug en Verhoeven,

en minister Opstelten van Veiligheid en Justitie, die vergezeld is van enkele ambtenaren van zijn ministerie.

Aanvang 19.05 uur

De **voorzitter**: Ik open dit algemeen overleg en heet eenieder van harte welkom. Mevrouw Gesthuizen komt iets later. Het doel van dit algemeen overleg is om te komen tot afspraken met de regering over de wijze van informatieverstrekking door de regering. We willen bovendien meer weten over het verloop van de onderhandelingen, de wetgevingsprocedure en een eventueel vervolgoverleg.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Dit is een heel technisch onderwerp, zodat we het kort houden. De behandeling zal plaatsvinden in de Telecomraad. Maar bij ons valt dit onderwerp onder de minister van Veiligheid en Justitie. Hoe gaat de Nederlandse regering daarmee om? Hoe moet het parlement daarmee volgens de minister omgaan?
Ik ben erg te spreken over het Nationaal Cyber Security Centrum (NCSC). Wil de regering het punt van de infrastructuur inbrengen in de uitvoering van de Europese richtlijn om zo versplintering te voorkomen? In hoeverre kunnen de kosten worden gedrukt?
De regering ziet privacyrisico's bij het delen van informatie over de aanvallen. Is het mogelijk de informatieplicht zo specifiek te maken dat er geen privacygevoelige informatie hoeft te worden gedeeld, maar alleen informatie die relevant is om de aanval te bestrijden?

De heer **Dijkhoff** (VVD): Voorzitter. Omdat dit onderwerp niet in de JBZ-Raad aan de orde komt, maar wel wordt besproken met de minister van Veiligheid en Justitie, past het niet om te vragen of we via de JBZ-Raad op de hoogte kunnen worden gehouden. Als we vier keer per jaar een update kunnen krijgen, hoeft dat niet per se te leiden tot een AO. Daarbij zouden we ook een link kunnen leggen met de Europese richtlijn voor dataprotectie. Als dat lukt, zou dat fijn zijn.
Ik heb nog een aantal aandachtspunten, waarvan ik hoop dat we daarvan op de hoogte worden gehouden en dat Nederland daarin een duidelijke inbreng heeft. Over het algemeen hoop ik dat die inbreng is samen te vatten in de woorden «lead by example». Het klinkt misschien een beetje arrogant, maar de indruk is namelijk dat Nederland vooroploopt met een aanpak die een goede balans kent tussen overheidsdwang en meldplichten enerzijds en een cultuur waarin bedrijven zaken uit zichzelf al melden anderzijds, zonder bang te zijn dat hun vuile was buiten komt te hangen na zo'n melding. Menig ander Europees land heeft nog niet eens een bureau om hiermee überhaupt om te gaan, en moet dus een been bijtrekken. Het voordeel is dat we ons model kunnen aanbieden om ervan te leren.
Waarover wij ons zorgen maken – wij willen deze punten graag terugzien in de rapportage – is bijvoorbeeld de breedte van de meldplicht. Door het niet maken van keuzes lijkt die meldplicht heel breed, waarbij ze ook nog door lidstaten kan worden uitgebreid. Wij hechten zeer aan een scheiding tussen een meldplicht voor vitale structuren en een stimulering van de meldbereidheid bij bedrijven.
Een ander punt is onze verhouding ten opzichte van de rest van de wereld en onze economische concurrentiepositie. Welke impact heeft het als we in de EU heel veel plichten opleggen die makkelijker te omzeilen zijn door

je te huisvesten in een ander land, waar veel minder plichten gelden? Ik noem de Verenigde Staten. Verder noem ik het risico van dubbele meldingen. Als een bedrijf in meerdere Europese landen opereert, is niet duidelijk of je met melding bij één computer emergency response team (CERT) klaar bent, of dat je dat zelf steeds moet melden. Dat betekent een flinke werklast voor mensen die die meldplicht krijgen opgelegd. Verder wordt een uitzondering gemaakt voor micro-ondernemingen. Welk criterium zal zich daarvoor ontwikkelen? Hierbij is een parallel met dataprotectie zichtbaar: er zijn allerlei modellen om dat te bepalen, van het aantal werknemers tot het aantal burgers waarvan je gevoelige informatie bezit. Dit heeft een grote impact op de bedrijven en de sectoren die daaronder vallen.
De huidige constructie oogt nog heel erg onschuldig: nationale lidstaten hebben een CERT en een autoriteit. Op Europees niveau vindt coördinatie via ENISA plaats, maar omdat veel landen niets of bijna niets doen op dit terrein, vrezen wij bij voorbaat dat bij die landen de neiging zal ontstaan om het dan maar Europees te regelen. Dan hoeven zij alleen maar te tekenen en eventueel te betalen. Dat zien wij niet graag gebeuren.

Voorzitter: Dijkhoff

De heer **Verhoeven** (D66): Voorzitter. We hebben vanmorgen twee technische briefings gehad over dit onderwerp. Cyberaanvallen zijn aan de orde van de dag. Banken kunnen erover meepraten. Vandaag stond in de krant dat China onze ambtenaren hackt, DigiD is vandaag ge-ddos't, en ook mediabedrijven en luchtvaartmaatschappijen zijn slachtoffer van deze aanvallen. Het geeft natuurlijk een enorm gevoel van onrust, maar we moeten ervoor waken alles op een hoop te gooien. De technieken en de dreigingen verschillen immers per geval naar aard en omvang. Zo is fishing al een relatief oude techniek, waarmee ze overigens nog niet ongevaarlijk is. Ddos-aanvallen zijn vooral gevaarlijk voor de beschikbaarheid van diensten, en niet zozeer voor de data die daarachter zitten. De echte risico's zijn toch vooral de inbraken door gaten in systemen of software.
We bespreken vandaag de Nederlandse inzet op het punt van de Europese richtlijn voor netwerk- en informatiebeveiliging. Die richtlijn gaat met name over inbraken en kent drie pilaren: de eerste is het voorbereid zijn, dus het beschikken over een CERT, een lokaal cybersecurityteam en een cyberstrategie. De tweede pijler is internationale samenwerking: kennisdeling, coördinatie en het omgaan met de infrastructuur die daarbij hoort. De derde pijler is het introduceren van een cultuur van risicomanagement. Is dit voldoende? Wat onze fractie betreft zitten er zeker goede zaken in. We kunnen grotendeels meegaan met de kabinetsreactie. Maar voor een goede analyse is het ook goed om het naar een iets hoger niveau te trekken. Allereerst moeten wat ons betreft alle betrokkenen hun eigen verantwoordelijkheid nemen: de gebruikers, de leveranciers en de installateurs. Laten we het eens vergelijken met een auto op de snelweg, wat deze minister moet aanspreken. De leverancier is verantwoordelijk voor de kwaliteit van de auto en een rijbewijs is nodig om de weg op te mogen. Een derde in de keten verzorgt de infrastructuur. Op die manier kijken we ernaar. Problemen moeten proportioneel worden aangepakt. Wij moeten dus niet gelijk in een stuip schieten en roepen om meer bevoegdheden of meer controleurs als er een keer wat gebeurt. Wij geloven veel meer in kleine, praktische maatregelen en niet direct overal camera's. Terug naar dat voorbeeld van die auto: je moet je auto gewoon op slot zetten, of een omleiding opzetten als het verkeer vastloopt.
De regering stelt in haar reactie voor om de voorgestelde meldplicht te verkleinen. Mijn fractie zou liever zien dat er een meeromvattende meldplicht komt. Elke organisatie die gehackt wordt, heeft blijkbaar iets van waarde. De inbraakinformatie is dus relevant. Wij doelen overigens

slechts op inbraken en niet op alle soorten cyberaanvallen. Anders zou je ook een melding moeten doen bij elke ddos-aanval en daar geloven wij niet in. Graag hoor ik van de minister waarom het kabinet deze keuze maakt.
Ik zeg ook kort iets over persoonsgegevens. De combinatie van artikel 15 met artikel 8 en overweging 39 maakt dat CERT's de bevoegdheid krijgen om privégegevens op te vragen bij bedrijven en die onderling uit te wisselen. De privacyregels worden dan niet van toepassing verklaard. Het lijkt mijn fractie beter om ervoor te zorgen dat de privacyregels wel van toepassing worden verklaard, zodat de verplichting bestaat om opgevraagde privégegevens waar mogelijk te verwijderen als blijkt dat er geen noodzaak is om ze op te vragen.
Mijn laatste punt gaat over de aansprakelijkheid. Inbraak verloopt vaak via een gaatje of gat in de software. Toch wordt zelden naar de leverancier gekeken. Kan de minister hierop ingaan? Kan hij aangeven of er in Europa enige discussie is over de aansprakelijkheid van softwareleveranciers?
Tot slot heb ik drie verzoeken, die volgens mij goed aansluiten bij de opmerkingen van de collega's Oosenbrug en Dijkhoff. Ik verzoek de minister om de Kamer op de hoogte te houden van de aanpassingen in het voorstel, om ons te informeren over wijzigingen in de Nederlandse inzet en om de Kamer met regelmaat op de hoogte te houden van de stand van zaken rondom dit voorstel.

Voorzitter: Verhoeven

De **voorzitter**: Mevrouw Gesthuizen is inmiddels ook gearriveerd. U hebt maximaal vijf minuten, mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP): Voorzitter. Op dit voorstel kan ik verheugd reageren. Bij netwerk- en informatiebeveiliging moet je je zeer bewust zijn van het feit dat er een buitenland bestaat, of dat nu binnen of buiten de Europese Unie is. Internet kent namelijk geen grenzen. In onze ICT-nota Knooppunten en oplossingen pleiten wij ervoor dat Nederland zowel in Europees verband als daarbuiten partners zoekt waarmee kan worden samengewerkt in deze strijd.
Ik begin met een algemene opmerking. Ik weet niet of wij als Nederland met dit voorstel echt verder komen en meer gaan doen aan de aanpak van problemen. Ik heb de indruk dat dit voorstel ook een beetje is ingediend om de achterblijvers onder onze hoede te nemen en ervoor te zorgen dat zij meegaan. Dat is op zich prima, maar wij moeten ons wel bewust zijn van het feit dat dit weer iets is wat in Nederland nog niet zo slecht gaat – wij zijn ons op dit moment in elk geval voldoende bewust van de risico's – maar wat in andere landen onvoldoende is. Daarom komt er een voorstel om anderen bij de les te houden. Het is maar een constatering. Soms denk ik dat er wel erg veel wetgeving is waarvoor dat geldt en vraag ik mij af hoe het zit met alle zegeningen die de Europese Unie voor ons land heeft.
Het tweede punt waarover nog niet volledig duidelijkheid bestaat, is het geld. Er is een redelijke inschatting te geven op basis van de beschikbare feiten, maar er is geen volkomen duidelijkheid over te geven. Ik neem aan dat wij erop mogen rekenen dat de Kamer onmiddellijk wordt geïnformeerd als zaken erg gaan afwijken.
Ik maak mij wat zorgen over de wijze van besluitvorming. Bij de conceptverordening en -richtlijnen voor dataprotectie hebben wij veel gedelegeerde besluitvorming gezien. Dat is hier ook het geval. Ik zie niet zo goed in hoe de minister daarop kan toezien en al helemaal niet hoe de minister daarover dan nog van gedachten kan wisselen met de Kamer. Deelt de minister die zorg? Ik ben er niet zo gelukkig mee als dit op grote schaal gebeurt, zeker niet als het gaat om dit soort onderwerpen, die zo in de actualiteit zijn dat zaken heel snel kunnen veranderen.

Ik heb ook een aantal concrete vragen. Welke instantie wil de Nederlandse regering gaan aanwijzen als bevoegde instantie voor de netwerk- en informatiebeveiliging? In het fiche lees ik dat Nederland van mening is dat een deel van de in de richtlijn voorgestelde maatregelen net zo goed op het niveau van de lidstaten kan worden geregeld. Over welke maatregelen heeft de minister het? Waarom kunnen die beter of net zo goed op nationaal niveau worden geregeld? Bedoelt de minister dat wij in zulke gevallen ook best bilateraal of met een klein groepje landen tot afspraken kunnen komen?
Tot slot heb ik een vraag over de privacy die aansluit bij de vraag van de heer Verhoeven. Ook mijn fractie vindt het belangrijk dat er oog is voor de privacy. Het is niet de bedoeling dat besloten wordt dat de privacyregels in dit geval even niet meer gelden. Of het nu gaat om verdachten of om mensen van wie de data op een andere manier in beeld komen, de richtlijn en de verordening over dataprotectie gelden hier evengoed. Er zijn gewoon regels die bepalen hoe je moet omgaan met privacy en hoe goed de privacybescherming moet zijn.

De **voorzitter**: De minister kan gelijk antwoorden.

Minister **Opstelten**: Voorzitter. Ik zal eerst een paar algemene punten aanstippen. Ik bedank de leden overigens voor hun constructieve opmerkingen. Ik heb niet de indruk dat wij ver uit elkaar liggen. Dat is belangrijk voor de start die wij nu maken. Cybersecurity is van groot belang. Elke dag is er wel iets. Ik zal niet alles herhalen. De verschillende incidenten in diverse vitale sectoren hebben de afgelopen maanden laten zien dat het van belang is om een extra stap te zetten. Die stap moeten wij in Nederland op publiek-privaat gebied zetten, maar ook internationaal. Daarom zitten wij hier vandaag. Een van de belangrijkste recente internationale ontwikkelingen op het terrein van cybersecurity is de in februari uitgekomen Europese cybersecuritystrategie en de in deze strategie genoemde netwerk- en informatiebeveiligingsrichtlijn, de NIB-richtlijn. De Europese onderhandelingen zijn pas net begonnen. Ik ben dan ook blij dat de Kamer mij vandaag heeft uitgenodigd. Dat is een goede timing. Het is van het grootste belang dat de Kamer goed wordt geïnformeerd over en betrokken bij het verdere verloop van de onderhandelingen en de positie die Nederland daarbij inneemt. Wij moeten hierover afspraken maken.
De NIB-richtlijn zet in op het toegenomen belang van Europese samenwerking op het gebied van informatiebeveiliging. Internationale samenwerking in het grensoverschrijdende domein van cybersecurity is vooral belangrijk op drie punten: opbouw van nationale capaciteit, coördinatie bij grensoverschrijdende incidenten en publiek-private samenwerking. Op deze punten moeten in EU-verband stappen worden gezet. Met de NIB-richtlijn zet de EU een extra stap en dat juich ik toe. De richtlijn moet aansluiten bij de ontwikkelingen die wij in Nederland reeds in gang hebben gezet. Ze passen bij het Nederlandse cybersecuritylandschap. Zo hebben wij het Nationaal Cyber Security Centrum, een goed functionerend Computer Emergency Response Team. De richtlijn voorziet erin dat ook andere Europese landen CERT-capaciteit opbouwen. Ook zijn wij in Nederland reeds begonnen met het uitwerken van de «security breach notification», overigens op verzoek van de Kamer. In mijn brief van 6 juli 2012 heb ik aangegeven dat de Europese ontwikkelingen en de meldplicht goed op elkaar moeten aansluiten. Dat zal ook de insteek zijn die wij in Europa kiezen.
Daarnaast zie ik in de richtlijn een aantal aandachtspunten die ook genoemd worden in het fiche dat wij in maart reeds naar de Kamer hebben gestuurd. Ik zal ze toch nog even noemen. Het eerste punt is het in stand houden en gebruikmaken van de bestaande Nederlandse structuren. Dat is essentieel. Er is daarbij geen overlap met nieuwe

EU-structuren. Het tweede punt is het respecteren van nationale verantwoordelijkheden. Mevrouw Gesthuizen zei daar al iets over. Het derde punt is het behouden van verantwoordelijkheden van de private sector. Het vierde punt is de borging van vertrouwelijkheid en privacy bij het uitwisselen van gegevens over incidenten binnen de Europese Unie. Ik denk dat wij elkaar daarin zouden kunnen naderen, maar dat moet blijken in het vervolg van de hele ontwikkeling. Het vijfde punt is het keihard beteugelen van de implementatiekosten. Wij moeten strak opereren. Dat zijn de vijf uitgangspunten en die schuren nadrukkelijk met het voorstel dat nu op tafel ligt. Zoals ik gezegd heb, vind ik het van groot belang om de Kamer goed te betrekken bij de nadere besluitvorming, des te meer omdat cybersecurity raakt aan alle facetten van het dagelijks leven.
Na de Telecomraad in juni 2013, waarbij de voortgang van de NIB-richtlijn op de agenda staat, zal ik de Kamer schriftelijk informeren. Daarbij zal ik in het bijzonder ingaan op de ontwikkeling van de Europese beraadslagingen, de positie van Nederland en eventuele wijzigingen van de standpunten die wij eerder hebben meegegeven in het BNC-fiche. Ik ben ervan overtuigd dat wij met deze aanpak de goede weg hebben gevonden. Dit is natuurlijk een dynamisch ontwikkelgebied.
Ik loop nu kort de vragen langs. Mevrouw Oosenbrug heeft erop gewezen dat ik zelf niet bij de Telecomraad aanwezig zal zijn. Zij vraag hoe wij hiermee omgaan. Wij zijn nauw betrokken bij de onderhandelingen in de voorbereidende werkgroep van de Telecomraad. In afstemming met mijn collega van EZ zal ik de Kamer informeren over de zaken die in de Telecomraad worden besproken en met de richtlijn te maken hebben. Ik vind het idee van de heer Dijkhoff wel goed. Wij zouden kunnen afspreken dat ik de Kamer viermaal per jaar, mede namens mijn collega's die op dit terrein betrokken zijn, een bericht stuur waarin alle wijzigingen en de Nederlandse inzet verwoord zijn. Als er aanleiding is om het anders te doen omdat er ineens iets is, dan zullen wij dat niet nalaten. Wij moeten hiermee praktisch omgaan. Ik heb het genoegen om met een aantal van de aanwezige leden ongeveer elke maand een AO JBZ-Raad te voeren. Wij kunnen daar altijd bekijken hoe wij dit agenderen. Wellicht kan een van de leden dan de bereidheid tonen om even aan te schuiven voor dit agendapunt. Zo zou het dus kunnen. De voortgang van de richtlijn wordt in de Telecomraad besproken. Deze Telecomraad vindt tweemaal per jaar plaats, bedenk ik mij nu. Ik zal de Kamer in elk geval na deze Raad informeren en indien nodig zal ik tussentijds informeren. Ik stel voor dat ik na de eerste Telecomraad een suggestie doe over de manier waarop wij het beste kunnen communiceren. Dat is de meest praktische werkwijze.
Mevrouw Oosenbrug heeft ook gesproken over privacyrisico's. Zij vraagt mij om de informatieplicht te beperken tot de informatie die nodig is om aanvallen te bestrijden. Het is van belang om alleen de noodzakelijke gegevens te verstrekken. IP-adressen worden gezien als persoonsgegevens. Wij beperken de informatie, maar delen wel IP-adressen om aanvallen te kunnen staken.
Verder heeft mevrouw Oosenbrug mij gevraagd om de bestaande infrastructuur van het NCSC in te brengen. Nederland heeft inderdaad al een goed functionerende overheids-CERT. Ook functioneert de beleidsdirectie van mijn ministerie al op het niveau van een nationale autoriteit. Nederland voldoet daarin dus al op hoofdlijnen aan de richtlijn. Dit zal de kosten zeker kunnen drukken. Ik ben bereid om dit model in de EU onder de aandacht te brengen.
De heer Dijkhoff en mevrouw Gesthuizen vrezen dat de landen in de voorhoede worden geremd in de ontwikkeling doordat men veel attentie ontwikkelt ten aanzien van de landen die nog niet zover zijn. De richtlijn is gericht op het bijtrekken van weinig ontwikkelde landen op het gebied van cybersecurity. Ik steun dat wel, want dit is in ons belang. Wel moeten wij voortbouwen op onze bestaande structuren. Bevoegdheden blijven nationaal. Meer samenwerking is belangrijk. De voorhoede bestaat uit

Nederland, het Verenigd Koninkrijk, Duitsland, Zweden en Frankrijk. Wij trekken die kar. Wij zullen zo veel mogelijk gezamenlijk optrekken. Wij moeten ook niet gehinderd worden in ons tempo, dus ik heb de opmerkingen hierover begrepen.

De **voorzitter**: De heer Dijkhoff wil u tussendoor een vraag stellen.

De heer **Dijkhoff** (VVD): Dit is wellicht een wat rare opmerking voor een Kamerlid, maar ik ben een beetje bang dat de minister nu al mijn vragen van een antwoord of reactie gaat voorzien. Een AO Behandelvoorbehoud is vaak een raar AO. Als er ontwikkelingen zijn op het gebied van de punten die ik heb aangedragen, zie ik graag dat die in de rapportages worden weergegeven. Kan de minister dat toezeggen? Ik hoef daar nu niet per se een antwoord op. Als er maar twee keer per jaar een Telecomraad is, kan de minister ook maar twee keer in plaats van vier keer per jaar rapporteren, want als er tussentijds niks te melden is, hoeven wij elkaar niet met papier te belasten. Ik zie dit echt als een procedureafspraak, na vandaag verlopend als behandelvoorbehoud. Officieel is een dergelijk AO ook niet bedoeld voor een inhoudelijke behandeling.

Minister **Opstelten**: Geldt dit voor alle leden? Ik kan mij dat voorstellen. In dat geval zeg ik toe dat ik alle punten meeneem in het proces en dat ik ze in de rapportages van antwoord zal voorzien.

De **voorzitter**: Wij gaan het inventariseren.

Mevrouw **Gesthuizen** (SP): Op zich is het heel prettig dat de minister onze punten gehoord heeft en dat hij ze meeneemt. Toch kan ik mij indenken dat er op bepaalde vlakken nog wel wat verschil is tussen de visie van de minister en onze visie. Ik heb niet heel veel vragen gesteld, maar zou het wel prettig vinden als ik daarop een kort antwoord kon krijgen.

De **voorzitter**: Mevrouw Oosenbrug? U vindt het goed, begrijp ik.
De minister noemde de borging van de privacy al als een van de aandachtspunten, maar ik zou toch graag nog antwoord krijgen op mijn vraag daarover. Verder zie ik wel iets in de opmerking van de heer Dijkhoff. Laten wij de minister vragen om in algemene zin in te gaan op de punten waarop veel licht zou kunnen zitten tussen de opvattingen van de minister en die van de leden, en laten wij verder vertrouwen op de rapportage. Ik zie dat dit breed gesteund wordt.

Minister **Opstelten**: In dat geval sla ik de vragen van de heer Dijkhoff verder over. Wij zullen al zijn punten meenemen.
De heer Verhoeven en mevrouw Gesthuizen hebben gevraagd op welke punten in de richtlijn Nederland kanttekeningen plaatst met betrekking tot privacy en vertrouwelijkheid bij de uitwisseling van gegevens over cyberrisico's en cyberdreigingen. Oog voor privacy is belangrijk. Nederland plaatst kanttekeningen bij de mate waarin bepaalde informatie überhaupt met andere lidstaten en de Commissie zou moeten worden gedeeld, dat is het kernpunt. Commissie vraagt in de richtlijn informatie over samenwerkingsplannen, incidentbehandelingsprocedures, meldingen bij nationale autoriteiten, incidentinformatie en audits van nationale marktpartijen. De richtlijn beschrijft niet hoe het samenwerkingsnetwerk en de Commissie met dergelijke deels vertrouwelijke informatie zullen omgaan. Wij staan dus nog aan het begin van veel vragen hierover.
Mevrouw Gesthuizen heeft zorgen over de dataprotectie en gedelegeerde besluitvorming. In de richtlijn staat gedelegeerde besluitvorming ten aanzien van het kiezen van informatie-uitwisselingssystemen en het

bepalen welke incidenten moeten worden gemeld. Dit moet mijns inziens nog verder worden uitgewerkt. Ik deel dus de zorg van mevrouw Gesthuizen hierover, evenals haar zorg op andere punten.
Komen wij verder met de richtlijn? Ja, die is noodzakelijk. Ik juich het toe dat uniformering gaat plaatsvinden. Welke bevoegdheden houden wij op nationaal niveau? Nederland wil graag met de Commissie bekijken welke risico's en incidenten tot een early warning moeten leiden. Het gaat om de manier waarop je dergelijke zaken met elkaar deelt, maar er moet wel iets preciezer worden bepaald in welke omstandigheden overheden en marktdeelnemers incidenten moeten melden. In de Nederlandse verhoudingen, met een publiek-private samenwerking, is dat een kwestie van precisie. Ik heb bijvoorbeeld net een gesprek gehad met de ceo's van de banken. Zij gaan een liaison bij het NCSC plaatsen, zodat wij continu geïnformeerd worden en niet zelf navraag moeten gaan doen. Men gaat permanent bij het centrum zitten. De vraag is uiteraard wel of wij dat internationaal ook op hetzelfde niveau willen delen.
Wij gaan nog bezien welke instantie in Nederland de bevoegde autoriteit zou zijn. Het ligt voor de hand dat dit de directie Cyber Security van mijn departement zou zijn. Als nationale CERT ligt het NCSC het meest voor de hand. Wij moeten als kabinet nog conclusies trekken, in overleg met de Kamer.
Daarbij wil ik het laten.

Mevrouw **Gesthuizen** (SP): Ik ben nog een vraag vergeten. Wij gaan meer samenwerken met landen in de EU, maar hoe gaan wij ermee om als er een aanval komt vanuit een derde land? In de richtlijn ontbreekt de visie daarop. Gaan wij in zo'n geval gezamenlijk melden aan dat derde land? Wordt dit helemaal overgelaten aan andere lidstaten? Hoe ziet de minister dat? Als dat niet in deze richtlijn geregeld wordt, moeten wij het later wellicht nog ergens regelen.

Minister **Opstelten**: Dank voor de vraag. Mijn eerste reactie zou zijn dat in zo'n geval in eerste instantie de nationale bevoegdheden gelden. Je moet natuurlijk afspraken maken over de manier waarop je hiermee omgaat.

Mevrouw **Gesthuizen** (SP): Dank u. Ik heb ook een vraag over handhaving. Ik neem aan dat die voor een belangrijk deel bij de Europese Commissie zal komen te liggen. Klopt dat?

Minister **Opstelten**: Als er al sprake is van handhaving op Europees niveau, zal die bij de Europese Commissie liggen. Het vertrekpunt is echter nationaal.

De **voorzitter**: Helder. Ik zie dat er geen verdere vragen zijn en zie dat er ook geen behoefte is aan een tweede termijn. Hebben enkele leden wellicht nog behoefte aan een nabrander?

Mevrouw **Oosenbrug** (PvdA): Ik heb begrepen dat wij hier ook zitten voor de voorhangprocedure. Wij zien heil in samenwerking op dit vlak. Wat mijn fractie betreft kan het behandelvoorbehoud worden opgeheven. Wij hebben gehoord dat wij op de hoogte worden gehouden en dat was het belangrijkste.

De **voorzitter**: Voor een goede besluitvorming in deze commissie is het belangrijk dat iedereen even aangeeft dat het behandelvoorbehoud kan worden opgeheven.

De heer **Dijkhoff** (VVD): Dat gebeurt sowieso na dit AO.

De **voorzitter**: Per definitie? Dat is dan geregeld.

Mevrouw **Gesthuizen** (SP): Dat lijkt mij ook, tenzij er nog een VAO zou worden aangevraagd door de PVV, die wellicht heel kritisch is over dit voorstel.

De **voorzitter**: Dan had die fractie hier misschien ook aanwezig kunnen zijn.
Ik lees de toezeggingen voor. De minister van Veiligheid en Justitie zal de Kamer vier keer per jaar informeren over de voortgang van de onderhandelingen. Dit is teruggebracht naar twee keer per jaar op basis van de frequentie waarop de Telecomraad samenkomt. Na de eerste Telecomraad komt de minister met een rapportagevoorstel. Voorts wordt de Kamer tussentijds geïnformeerd indien dat noodzakelijk is, dus bij bijzonderheden. Bij de rapportage zal de minister ingaan op de punten die de leden tijdens dit AO hebben ingebracht.

De heer **Dijkhoff** (VVD): De minister deed een suggestie om overbodige AO's te voorkomen. Wij worden standaard twee keer per jaar geïnformeerd en als dat nodig is ook tussentijds. De minister stelde voor om een bespreking, als daaraan behoefte is, te koppelen aan het AO JBZ-Raad, dat toch al bijna maandelijks geagendeerd wordt.

De **voorzitter**: Ik denk dat dit breed gedeeld wordt door de commissie. Laten wij dat afspreken.
Ik dank de minister en zijn mensen voor de antwoorden, de collega's voor hun inbreng en iedereen die heeft meegekeken voor zijn aandacht.

Sluiting 19.44 uur.