Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

36 084 Wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders

Nr. 8 **NOTA NAAR AANLEIDING VAN HET VERSLAG**

Ontvangen 8 juli 2022

Met belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Digitale Zaken over het wetsvoorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Ik dank de commissie voor de snelle vaststelling van dit verslag. In deze nota beantwoord ik de door de commissie gestelde vragen. Daarnaast maak ik graag van de gelegenheid gebruik om op enkele punten een nadere toelichting te geven. Bij de beantwoording heb ik de volgorde van het verslag aangehouden. Voor de leesbaarheid is de inbreng van de fracties cursief afgedrukt. Ik hoop de vragen genoegzaam te hebben beantwoord en hoop op een spoedige voortzetting van de behandeling van dit wetsvoorstel.

I. ALGEMEEN DEEL

1. Inleiding

De leden van de VVD-fractie merken op dat de behandeling van deze wetswijziging bij de Minister van Justitie en Veiligheid ligt, maar dat het toezicht van deze wijziging bij de Minister van Economische Zaken en Klimaat ligt. Kan de regering uiteenzetten hoe de verdeling van taken en verantwoordelijkheden ligt bij de Ministers en of er knelpunten worden ervaren?

Het klopt dat dit wetsvoorstel door mij in procedure is gebracht en dus inmiddels ook bij uw Kamer is ingediend. Dit wetsvoorstel bevat namelijk een tweetal wijzigingen van de Wbni, waarvan de Minister van Justitie en Veiligheid de primair verantwoordelijk bewindspersoon is. Deze wijzigingen betreffen ook de taken en bevoegdheden die krachtens genoemde wet aan de Minister van Justitie en Veiligheid toekomen én die in de

kst-36084-8
ISSN 0921 - 7371
's-Gravenhage 2022

praktijk door het Nationaal Cyber Security Centrum (hierna: NCSC) worden uitgeoefend. Het toezicht op de uitoefening door het NCSC van die taken en bevoegdheden geschiedt, voor zover het daarbij gaat om de verwerking van persoonsgegevens, door de Autoriteit Persoonsgegevens (hierna: AP). De inhoud van dit wetsvoorstel is afgestemd met de andere betrokken bewindspersonen, waaronder de Minister van Economische Zaken en Klimaat. Van een andere betrokkenheid van die bewindspersonen ten aanzien van dit wetsvoorstel is, anders dan de leden van de VVD-fractie veronderstellen, geen sprake.

Ten aanzien van de verdeling van de verschillende in de Wbni geregelde taken en bevoegdheden merk ik op dat hierin met dit wetsvoorstel geen wijziging wordt gebracht, mede ook omdat tot op heden hierover geen knelpunten worden ervaren. De Minister van Justitie en Veiligheid is op basis van de Wbni belast met het verlenen van bijstand aan vitale aanbieders en rijksoverheidsorganisaties bij digitale dreigingen en incidenten en het daartoe verrichten van analyses. Bij het doen van die analyses kan dreigings- en incidentinformatie beschikbaar komen die relevant is voor aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid (hierna: andere aanbieders). De Minister is op grond van de Wbni ook belast met het verstrekken van die informatie aan zogeheten schakelorganisaties van andere aanbieders als bedoeld in artikel 3, tweede lid, van de Wbni. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten. Onder schakelorganisaties vallen onder meer computercrisisteams en organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT's).

De betrokken vakministers zijn krachtens deze wet belast met het houden van het toezicht op de naleving van hierin geregelde verplichtingen (zoals de zorgplicht) door vitale aanbieders die als aanbieder van essentiële diensten zijn aangewezen. Zo geschiedt het toezicht op energiebedrijven door het Agentschap Telecom namens de Minister van Economische Zaken en Klimaat.

Deze leden volgen de ontwikkelingen omtrent de richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn) op de voet. Kan de regering uiteen zetten of en welke gevolgen dit gaat hebben voor de uitvoering van deze wet?

Over de herziening van de NIB-richtlijn hebben de EU-lidstaten en het Europees Parlement op 13 mei 2022 een voorlopig politiek akkoord bereikt. Naar verwachting wordt de richtlijn in het najaar van 2022 definitief vastgesteld waarna de richtlijn moet worden geïmplementeerd in nationale wetgeving. Deze implementatie zal gevolgen hebben voor de Wbni, bijvoorbeeld vanwege de toename van het aantal aanbieders dat onder de toepasselijkheid daarvan zal komen te vallen.

De leden van de PVV-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en hebben nog enkele vragen en opmerkingen over het wetsvoorstel. Deze leden signaleren dat de Afdeling Advisering van de Raad van State van mening is dat in het wetsvoorstel onvoldoende wettelijk is gewaarborgd dat schakelorganisaties het vereiste niveau van beveiliging en privacybescherming hebben op het moment dat zij worden aangewezen. Toch ziet de regering geen reden beveiligingsverplichtingen voor organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's) in de wet op te nemen. Deze leden vragen waarom de regering

van dit advies is afgeweken en hoe nu kan worden gegarandeerd dat de schakelorganisaties aan het vereiste niveau van beveiliging en privacybescherming (blijven) voldoen.

De beveiligingsverplichtingen waar de Afdeling advisering van de Raad van State in haar advies naar verwijst, betreffen de verplichtingen uit hoofdstuk 4 van de Wbni. Deze verplichtingen betreffen de implementatie van de NIB-richtlijn en hebben alleen betrekking op vitale aanbieders die hun diensten verlenen binnen in die richtlijn limitatief opgesomde sectoren (aanbieders van essentiële diensten). In het Besluit beveiliging netwerk- en informatiesystemen worden deze vitale aanbieders als zodanig aangewezen. Wat betreft de sectoren gaat het onder meer om de sectoren energie (met de subsectoren elektriciteit, gas en aardolie), vervoer (met de subsectoren luchtvervoer, spoorvervoer, vervoer over water en wegvervoer), drinkwater en het bankwezen. Wat betreft de daarbinnen aangewezen vitale aanbieders gaat het onder meer om drinkwaterbedrijven, de Nederlandse Aardolie Maatschappij B.V. en de netbeheerder van het landelijk hoogspanningsnet. Er is geen reden gezien om de verplichtingen die op deze vitale aanbieders van toepassing zijn, ook van toepassing te verklaren op andere aanbieders of hun schakelorganisaties. De continuïteit van hun dienstverlening wordt namelijk niet in dezelfde mate van belang geacht voor de Nederlandse samenleving en de aantasting van bijvoorbeeld de beschikbaarheid van die dienstverlening is in mindere mate maatschappelijk ontwrichtend. Meer concreet: wanneer de beschikbaarheid van de dienstverlening van bijvoorbeeld een als vitaal aangemerkt drinkwaterbedrijf of netbeheerder van het landelijk hoogspanningsnet wordt aangetast, dan is dat in grotere mate maatschappelijk ontwrichtend dan wanneer dat gebeurt met de dienstverlening van een niet-vitale aanbieder of diens schakelorganisatie.

Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten. Zij zijn het meest bekend met de in hun achterban aanwezige netwerk- en informatiesystemen, bijbehorende belangen en risico's en informatiebehoeften. Onder schakelorganisaties vallen onder meer zogeheten organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT). Om te garanderen dat de schakelorganisaties aan het vereiste niveau van beveiliging en het vertrouwelijk behandelen van gegevens voldoen, zijn er voor én na de aanwijzing als OKTT verschillende waarborgen. Voordat een schakelorganisatie krachtens artikel 3, tweede lid, van de Wbni als OKTT wordt aangewezen wordt een grondige beoordeling verricht. Met deze beoordeling wordt bepaald of de verstrekking door het NCSC van de in dat artikel bedoelde informatie aan die schakelorganisatie verantwoord en gerechtvaardigd is. In het kader daarvan wordt onder meer, op basis van de uitkomsten van een navraag hiernaar bij de betrokken schakelorganisatie, getoetst of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen met betrekking tot de netwerk- en informatiesystemen heeft genomen en hierdoor geacht kan worden de van het NCSC ontvangen informatie zorgvuldig te verwerken en de vertrouwelijkheid van deze informatie voldoende te waarborgen. Ook wordt, op basis van diezelfde navraag, beoordeeld of de betrokken schakelorganisatie afdoende maatregelen heeft genomen om persoonsgegevens rechtmatig te verwerken. Tevens wordt beoordeeld of de organisatie een voldoende afgebakende doelgroep heeft van aanbieders die (in hoofdzaak) niet vitaal zijn en geen deel uitmaken van de rijksoverheid. Verder wordt beoordeeld of de van het NCSC te ontvangen informatie niet voor andere doeleinden wordt gebruikt dan het informeren en adviseren van aanbieders in hun doelgroep. Deze beoordeling zal na de inwerkingtreding van de in dit

wetsvoorstel voorgestelde wijzigingen uiteraard ook blijven plaatsvinden bij de aanwijzing van een schakelorganisatie als OKTT.

Pas nadat een schakelorganisatie deze grondige beoordeling heeft doorstaan kan de organisatie worden aangewezen als OKTT. In dat geval moet die schakelorganisatie een verklaring ondertekenen waarin is opgenomen dat aan het NCSC melding wordt gemaakt van onder meer belangrijke wijzigingen van de getroffen (technische en organisatorische) beveiligingsmaatregelen of van de doelgroep en de taken die ten behoeve van die doelgroep worden verricht. Indien er op basis van een dergelijke melding aanwijzingen zijn voor bijvoorbeeld een onvoldoende vertrouwelijke omgang door een schakelorganisatie met gegevens, dan kan het NCSC het delen van informatie met die organisatie opschorten. Ook kan de aanwijzing als OKTT worden ingetrokken als uit verdere navraag blijkt dat niet meer aan de toetsingscriteria wordt voldaan. Het is echter niet zo dat het NCSC alleen het al dan niet doen van de hiervoor bedoelde melding door een OKTT afwacht. Het NCSC kan ook door informatie uit andere bronnen aanwijzingen krijgen dat een OKTT bijvoorbeeld onvoldoende vertrouwelijk omgaat met gegevens. Ook dan kan het NCSC de hiervoor genoemde acties ondernemen.

Voor schakelorganisaties geldt voorts uiteraard, als het gaat om de verwerking van persoonsgegevens na de ontvangst daarvan van het NCSC, dat zij dienen te voldoen aan de daaraan gestelde eisen op grond van de Algemene verordening gegevensbescherming (hierna: AVG) en dat op de naleving daarvan toezicht wordt gehouden door de AP. Als een OKTT de AVG schendt, dan kan de AP dus een handhavingstraject starten.

Naar het oordeel van de regering wordt hiermee, ook met inachtneming van de onderscheidenlijke verantwoordelijkheden van de verstrekker van en de ontvanger van informatie, in voldoende mate gewaarborgd dat de verstrekking door het NCSC van de in de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni bedoelde informatie alleen geschiedt aan schakelorganisaties die onder meer adequate maatregelen hebben getroffen voor een vertrouwelijke omgang met die informatie.

De leden van de CDA-fractie hebben met instemming kennisgenomen van het onderhavige wetsvoorstel. Deze leden hebben naar aanleiding hiervan geen vragen.

De leden van de SP-fractie hebben het voorstel voor wijziging van de Wet beveiliging- en informatiesystemen gelezen en hebben hierover nog enkele vragen en opmerkingen. Deze leden maken van de gelegenheid gebruik eerst een opmerking te maken over het doorlopen proces. De regering heeft verzocht vooruit te kunnen lopen op deze wetswijziging vanwege de toenemende digitale dreiging door de oorlog in Oekraïne. Hoewel deze leden deze digitale dreiging erkennen, zijn zij verbaasd over deze argumentatie. Er is veelvuldig door verschillende organisaties gewaarschuwd voor digitale dreigingen, onder meer door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Daarbij zijn er inmiddels meerdere aanvallen geweest, ook al in eerdere jaren. Waarom heeft deze wijziging dan zo lang op zich laten wachten?

Krachtens de Wbni kan het NCSC bepaalde dreigings- en incidentinformatie, die beschikbaar is gekomen bij analyses ten behoeve van de primaire taak van het NCSC (bijstand aan vitale aanbieders en rijksoverheidsorganisaties) én betrekking heeft op netwerk- en informatiesystemen van andere aanbieders, verstrekken aan schakelorganisaties van die andere aanbieders. Op dit moment kan het NCSC de hiervoor bedoelde informatie lang niet altijd delen met die andere aanbieders of met hun

schakelorganisaties, omdat de Wbni nog niet in deze bevoegdheid voorziet. Hierbij is het van belang om voor ogen te hebben dat aanbieders uiteraard primair zelf verantwoordelijk zijn voor het treffen van maatregelen ter beveiliging van hun netwerk- en informatiesystemen om daarmee de negatieve gevolgen van dreigingen of incidenten voor de continuïteit van hun diensten te voorkomen of de gevolgen daarvan zo veel mogelijk te beperken. Daartoe is het wel van belang dat aanbieders zo veel als mogelijk de beschikking hebben over voor hen relevante dreigings- en incidentinformatie. De afgelopen jaren is in *toenemende* mate sprake van (geslaagde) digitale aanvallen op andere aanbieders. Niet alleen het aantal (geslaagde) digitale aanvallen neemt toe, maar ook de ernst daarvan. Hierdoor is het oplossen van het ontbreken van de hiervoor bedoelde bevoegdheid urgent geworden. Vanwege de urgentie is dit voorstel met voorrang opgepakt.

De leden van de GroenLinks-fractie zien cybersecurity als randvoorwaarde van een digitaliserende samenleving en overheid, en het uitwisselen van informatie is hier onderdeel van. Maar bij meer verantwoordelijkheden, hoort ook gepast toezicht en gepaste verantwoordingsmechanismen. Deze leden zien dat de groei in digitale aanvallen op «andere aanbieders» gelijk gaat met een groeiende afhankelijkheid van meer aanbieders en minder ICT-leveranciers.

De leden van de Volt-fractie hebben met interesse kennisgenomen van het wetsvoorstel tot Wijziging van de Wet beveiliging netwerk- en informatiesystemen. Dit wetsvoorstel komt tegemoet aan een wens om organisaties en bedrijven beter op de hoogte te kunnen brengen van dreigingssituaties, met als doel de cyberweerbaarheid van Nederland te vergroten. Dat kan alleen met de juiste waarborgen. Over het wetsvoorstel hebben deze leden dus nog enkele vragen.

2. Aanleiding voor het wetsvoorstel

De leden van de GroenLinks fractie vragen of het begrip «andere aanbieders» voldoende afgebakend is in de voorgestelde wetswijziging.

De regering is van mening dat de beschrijving van de andere aanbieders, bedoeld in het voorgestelde artikel 3, tweede lid, onder e, van de Wbni, voldoende afgebakend is. Deze voorgestelde bepaling kent namelijk de volgende objectieve cumulatieve criteria:

1. de betrokken aanbieder is geen vitale aanbieder en evenmin een onderdeel van de rijksoverheid;
2. er is geen schakelorganisatie (dit is een organisatie die de taak heeft om aanbieders in zijn achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten) die de aanbieder kan voorzien van de informatie over dreigingen en incidenten met betrekking tot zijn netwerk- en informatiesystemen; en
3. er is sprake van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.

3. Inhoud van het wetsvoorstel

3.1 Delen van dreigings- en incidentinformatie met andere aanbieders

De leden van de VVD-fractie vragen of de regering kan toelichten of bedrijven zoals grote toeleveranciers van firewalls ook onder «andere aanbieders» zouden kunnen vallen.

Om een aanbieder te kwalificeren als een aanbieder als bedoeld in het voorgestelde artikel 3, tweede lid, onder e, van de Wbni, moet zijn voldaan aan de volgende cumulatieve criteria, die hierboven in antwoord op een vraag van de leden van de GroenLinks-fractie, ook reeds zijn genoemd:

1. de betrokken aanbieder is geen vitale aanbieder en evenmin een onderdeel van de rijksoverheid;
2. er is geen schakelorganisatie die de aanbieder kan voorzien van de informatie over dreigingen en incidenten met betrekking tot zijn netwerk- en informatiesystemen; en
3. er is sprake van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.

Het Digital Trust Center (hierna: DTC) is een schakelorganisatie voor het Nederlandse niet-vitale bedrijfsleven. Nederlandse toeleveranciers van grote firewalls vallen onder de doelgroep van deze schakelorganisatie. Deze schakelorganisatie kan hen dus voorzien van informatie over dreigingen en incidenten. Aangezien er bij deze bedrijven wél sprake is van een schakelorganisatie die hen kan voorzien van dreigings- en incidentinformatie, vallen zij dus niet onder de in artikel 3, tweede lid, onder e, Wbni bedoelde andere aanbieders.

De leden van de SP-fractie zien het belang van het voortijdig informeren van bedrijven en andere belanghebbenden in het geval van een digitale dreiging. Deze leden hebben daarom zelf gepleit voor de oprichting van het Digital Trust Center (DTC). Deze leden zien echter ook het gevaar dat er veel werk dubbel wordt gedaan, of werk blijft liggen omdat geen van de organisaties zich verantwoordelijk voelt, of organisaties zelfs elkaar gaan tegenwerken. Waarom is er niet gekozen voor één verantwoordelijke organisatie?

Er is niet gekozen voor één verantwoordelijke organisatie vanwege de volgende stelselinrichting en taakverdeling. Het NCSC heeft primair de taak om rijksoverheidsorganisaties en vitale aanbieders te informeren en adviseren over voor hen belangrijke dreigingen en incidenten. Daarnaast kan het NCSC dreigingsinformatie, die is verkregen in het kader van de primaire taakuitoefening én relevant is voor andere aanbieders, aan krachtens de Wbni aangewezen schakelorganisaties ten behoeve van die andere aanbieders verstrekken. Eén van die schakelorganisaties is het DTC. Het DTC heeft de taak om het niet-vitale bedrijfsleven, mede op basis van de informatie die van het NCSC wordt verkregen, te informeren en adviseren over digitale dreigingen en incidenten. Het NCSC en het DTC hebben dus duidelijk onderscheidenlijke primaire doelgroepen van organisaties waaraan informatie en advies over concrete dreigingen en incidenten wordt verstrekt. Door deze inrichting en taakverdeling wordt er geen dubbel werk gedaan, kan er geen verwarring ontstaan over van welke overheidsinstantie een aanbieder informatie en advies zal ontvangen. Van tegenwerking zal geen sprake zijn.

De leden van de GroenLinks-fractie vinden het opmerkelijk dat informatie van «andere aanbieders» die nu verkregen wordt «rest data» of «bijvangst» genoemd wordt. Betekent dit dat het Nationaal Cyber Security Centrum (NCSC) niet op zoek was naar gegevens over «andere aanbieders», maar dit nu toevallig tegenkomt? Hoe past dit in de principes van doelbinding en dataminimalisatie van de Algemene verordening gegevensbescherming (AVG)?

De door de leden van de GroenLinks-fractie bedoelde data betreft inderdaad telkens informatie over digitale dreigingen en incidenten die is verkregen bij analyses die worden uitgevoerd ten behoeve van de primaire taak van het NCSC. Die taak betreft het verstrekken van informatie en advies over digitale dreigingen en incidenten aan vitale aanbieders en rijksoverheidsorganisaties, zodat zij op basis daarvan maatregelen kunnen nemen om de continuïteit van hun dienstverlening te waarborgen en zodoende maatschappelijke ontwrichting te voorkomen. Deze taak is geregeld in artikel 3, eerste lid, van de Wbni. Het tweede lid van dit artikel bepaalt dat het NCSC óók de taak heeft om bij genoemde analyses over digitale dreigingen en incidenten betreffende andere aanbieders beschikbaar gekomen data te verstrekken aan de hierin opgenomen schakelorganisaties van die aanbieders. Het NCSC heeft deze taak ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland. De Wbni voorziet dus al, naast de taak van het verlenen van bijstand aan de primaire doelgroep, in de taak van het verstrekken van de hiervoor bedoelde data aan genoemde schakelorganisaties; in dit wetsvoorstel wordt voorgesteld om de in het kader van die taak ontvangende groep uit te breiden met andere aanbieders waarvoor geen schakelorganisatie aanwezig is.

Op grond van het doelbindingsbeginsel van artikel 5, eerste lid, onder b, van de AVG moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen zij vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Zoals gezegd wordt voorgesteld dat het NCSC ook de taak heeft om de hiervoor bedoelde data te verstrekken aan de in het voorstel bedoelde andere aanbieders, met als doel om die aanbieders in staat te stellen maatregelen te treffen om de continuïteit van hun dienstverlening te waarborgen of herstellen en daarmee nadelige maatschappelijke gevolgen te voorkomen. De voorgestelde verstrekking is noodzakelijk om dat doel te realiseren. Zonder de hiervoor bedoelde data weten andere aanbieders immers niet dat hun netwerk- en informatiesystemen kwetsbaar zijn of worden aangevallen en kunnen zij hier geen maatregelen tegen treffen. Hiermee valt de voorgestelde verstrekking binnen de kaders van het doelbindingsbeginsel.

Het beginsel van minimale gegevensverwerking houdt onder meer in dat persoonsgegevens ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt («dataminimalisatie»). Zonder persoonsgegevens als IP-adressen, domeinnamen en e-mailadressen van gebruikers van kwetsbare systemen of van aanvallers, is de verstrekking van dreigings- en incidentinformatie voor aanbieders niet zinvol. Zij kunnen dan namelijk niet bepalen welke van hun netwerk- en informatiesystemen kwetsbaar of al getroffen zijn en welke maatregelen genomen zouden moeten worden om dreigingen weg te nemen of incidenten te verhelpen. Er wordt uiteraard niet meer dreigings- en incidentinformatie aan andere aanbieders verstrekt dan noodzakelijk is; zij zullen alleen de voor hen relevante informatie krijgen zodat zij maatregelen kunnen nemen om digitale incidenten te voorkomen of de gevolgen daarvan te beperken. Hiermee wordt gehandeld binnen de kaders van het beginsel van dataminimalisatie.

De leden van de Volt-fractie merken allereerst op dat de definitie «andere aanbieders» erg ruim is. Hierdoor wordt het in theorie mogelijk om alle bedrijven en organisaties in Nederland te informeren. Dat betekent tegelijkertijd dat er een omvangrijke verwerkingsgrondslag wordt gecreëerd. Daarover maken deze lezen zich, in lijn met de Autoriteit Persoonsgegevens, zorgen. De bepaling is onvoldoende gespecificeerd en daarmee onvoldoende kenbaar en voorzienbaar, zoals wordt bedoeld in

rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), zeker nu er nog geen besluit is genomen waarin de OKTT's worden aangewezen. Kan de regering toelichten welke aanbieders zij voor ogen heeft met dit wetsvoorstel? Kan dit nader gespecificeerd worden, wellicht niet op individueel niveau, maar wel op het niveau van categorieën? Is er vanuit het verleden kennis opgebouwd over het type aanbieders dat met dit wetsvoorstel beoogd wordt? Zo ja, welk type aanbieder is dit? Wat bedoelt de regering concreet met «andere aanbieders»?

De in dit wetsvoorstel vervatte aanvulling van artikel 3, tweede lid, Wbni, met een nieuw onderdeel e maakt het NCSC bevoegd om in specifieke gevallen dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, te verstrekken aan aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid. In bovenbedoeld nieuw onderdeel is de daarin geregelde bevoegdheid tot verstrekking bovendien beperkt tot de gevallen waarin een aanbieder geen schakelorganisatie heeft waar deze aanbieder informatie van kan ontvangen én de informatie een dreiging of incident betreft die aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening. Hiermee wordt de reikwijdte van deze bevoegdheid voldoende specifiek omschreven. Van een omvangrijke uitbreiding van de bevoegdheid om informatie aan individuele aanbieders te verstrekken is hiermee ook geen sprake. Voor deze bevoegdheid geldt dan ook dat die, in samenhang met artikel 17, eerste lid, Wbni, voldoende bij wet voorzienbaar is. Tegelijk laat de bevoegdheid voldoende ruimte om aan aanbieders, die op dat moment nog geen of juist niet meer een schakelorganisatie hebben, belangrijke dreigings- of incidentinformatie te verstrekken en daarmee nadelige maatschappelijke gevolgen te voorkomen. Het NCSC heeft voldoende beeld van welke andere aanbieders momenteel geen schakelorganisatie hebben en waaraan dus krachtens artikel 3, tweede lid, onder e, van de Wbni informatie kan worden verstrekt in geval van dreigingen of incidenten met (mogelijke) aanzienlijke gevolgen. Voorbeelden van zulke aanbieders zijn politieke partijen en veiligheidsregio's.

Uit het bovenstaande volgt ook dat het voorgestelde artikel 3, tweede lid, onderdeel e, Wbni het dus niet mogelijk maakt om alle bedrijven en organisaties in Nederland over digitale dreigingen en incidenten te informeren. Zo geldt bijvoorbeeld voor alle niet-vitale bedrijven dat zij met het DTC een eigen schakelorganisatie hebben. Het DTC is krachtens de Wbni aangewezen als OKTT en informatieverstrekking ten behoeve van die bedrijven zal daarom dus telkens door tussenkomst van het DTC plaatsvinden.

3.2 Delen van vertrouwelijke herleidbare gegevens over aanbieders met OKTT's

De leden van de PVV-fractie hebben kennisgenomen van de verwachting van de regering dat de wijzigingen geen aanpassingen van ICT-systemen zouden vergen. Wel moeten een aantal werkprocessen worden aangepast. De leden vragen of dit ook geldt voor de OKTT's. Volgens de regering zijn er geen financiële gevolgen voor de OKTT's, omdat het aan deze partijen zelf is om te bepalen hoe zij omgaan met de ontvangen dreigings- en incidentinformatie. De leden vragen of de regering wel voorbereid is op eventuele logistieke en financiële ondersteuning van OKTT's.

Zoals opgenomen in de memorie van toelichting hebben de voorgestelde wijzigingen geen financiële gevolgen voor de OKTT's. Evenmin zijn er financiële gevolgen voor de aanbieders in de doelgroepen van die OKTT's waarop deze gegevens betrekking hebben. Het is aan deze partijen om zelf te bepalen hoe zij met de ontvangen dreigings- en incidentinformatie

omgaan. Mede hierom wordt er geen logistieke en financiële ondersteuning voor OKTT's voorzien. Overigens heeft het DTC wel een subsidieregeling voor cybersecurityinitiatieven en samenwerkingsverbanden ter verhoging van de cyberweerbaarheid van niet-vitale bedrijven in Nederland.

De leden van de VVD-fractie lezen dat de regering geen aanleiding ziet om beveiligingsverplichtingen voor OKTT's in de wet op te nemen. Welke negatieve gevolgen ziet de regering om deze beveiligingsverplichtingen in de wet op te nemen?

Het is naar mijn oordeel inderdaad niet aangewezen om ten aanzien van schakelorganisaties als OKTT's beveiligingsverplichtingen in de Wbni op te nemen. Voor het antwoord op deze vraag verwijs ik graag naar mijn eerder gegeven antwoord op de eerste vraag van de PVV-fractie.

De leden van de GroenLinks-fractie vragen of de regering nader kan definiëren welke organisaties zij als OKTT's ziet. Is dit bijvoorbeeld altijd een stichting?

Voor de ministeriële aanwijzing als OKTT komen alleen organisaties in aanmerking die bijvoorbeeld blijkens statuten of een wettelijk voorschrift, en daarmee objectief kenbaar, de taak hebben om andere aanbieders binnen hun doelgroep over digitale dreigingen of incidenten te informeren. De meeste organisaties die als OKTT zijn aangewezen zijn privaatrechtelijke organisaties, maar daarvan hoeft op zich dus niet sprake te zijn. Een voorbeeld hiervan betreft het DTC, onderdeel van het Ministerie van Economische Zaken en Klimaat, dat tot taak heeft om het niet-vitale bedrijfsleven over digitale dreigingen en incidenten te informeren en adviseren.

Waarom is er gekozen om OKTT's aan te wijzen per ministeriele aanwijzing, in plaats van ministeriele regeling?

Dit verschil in wijze van aanwijzing tussen computercrisisteams (ministeriële regeling) en OKTT's (besluit) was bij de totstandkoming van de wet geen bewuste keuze. Ik constateer dat er geen aanleiding is om OKTT's op een andere wijze aan te wijzen dan computercrisisteams. Zij hebben een in belangrijke mate vergelijkbare rol als het gaat om het delen van informatie met hun achterban. Bovendien zijn de eisen en voorwaarden die worden gesteld aan de aanwijzing van een organisatie als OKTT of als computercrisisteam al vrijwel gelijk aan elkaar. Daarom stel ik voor dat OKTT's en computercrisisteams beide op gelijke wijze worden aangewezen, namelijk bij ministeriële regeling.

Deze leden lezen dat er bij het aanwijzen van een OKTT getoetst wordt of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen met betrekking tot de netwerk- en informatiesystemen hebben genomen. Wordt dit na deze initiële toets, daarna stelselmatig gecontroleerd? Zo ja, door wie?

Na de aanwijzing als OKTT vindt geen stelselmatige controle plaats hiernaar. Naar het oordeel van de regering zijn er echter voldoende waarborgen op dit punt, zowel voor als na de aanwijzing als OKTT. Ik verwijs hierbij naar mijn antwoord op de eerste vraag van de PVV-fractie, waaruit niet alleen volgt dat er voorafgaand aan de aanwijzing van een organisatie als OKTT een grondige beoordeling plaatsvindt, maar er ook op wordt gewezen dat het NCSC de informatiedeling aan die OKTT kan opschorten en de aanwijzing kan intrekken als blijkt dat een OKTT bijvoorbeeld onvoldoende vertrouwelijk omgaat met gegevens. Verder

geldt voor schakelorganisaties uiteraard, als het gaat om de verwerking van persoonsgegevens na de ontvangst daarvan van het NCSC, dat zij dienen te voldoen aan de daaraan gestelde eisen op grond van de AVG en dat op de naleving daarvan toezicht wordt gehouden door de AP.

Ook lezen deze leden dat er wordt beoordeeld of de betrokken schakelorganisatie afdoende maatregelen heeft genomen om persoonsgegevens rechtmatig te verwerken. Door wie wordt dit beoordeeld? Is dit wellicht een taak voor de Autoriteit Persoonsgegevens, die de kennis en kunde hebben hiervoor?

Vóór de aanwijzing van een organisatie als OKTT vindt een grondige beoordeling plaats. In het kader daarvan wordt onder meer getoetst of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen met betrekking tot de netwerk- en informatiesystemen heeft genomen en hierdoor geacht kan worden de van het NCSC ontvangen informatie zorgvuldig te verwerken en de vertrouwelijkheid van deze informatie voldoende te waarborgen. Ook wordt, op basis van diezelfde navraag, beoordeeld of de betrokken schakelorganisatie afdoende maatregelen heeft genomen om persoonsgegevens rechtmatig te verwerken. Deze beoordeling wordt gedaan door het NCSC en de NCTV van mijn ministerie. Als het gaat om de verwerking van persoonsgegevens na de ontvangst daarvan van het NCSC geldt dat OKTT's moeten voldoen aan de daaraan gestelde eisen op grond van de AVG. De AP ziet toe op de naleving van de AVG. Graag verwijs ik hierbij tevens naar mijn antwoord op de eerste vraag van de leden van de PVV-fractie.

Waarom is deze grote hoeveelheid organisaties die geen vitale aanbieder of aanbieder is die onderdeel is van de rijksoverheid, niet aangesloten bij een, bij minsteriele regeling aangewezen, computercrisisteam? Hoe voorkomt de regering dat er overlap in verantwoordelijkheden komt door de toename van schakelorganisaties die als OKTT of computercrisisteam worden aangewezen?

Andere aanbieders zijn zelf primair verantwoordelijk om voldoende beveiligingsmaatregelen te nemen met betrekking tot hun netwerk- en informatiesystemen. Wel kunnen deze aanbieders ervoor kiezen om een schakelorganisatie in het leven te roepen, die hen daartoe van informatie en advies daarover voorzien. Dergelijke schakelorganisaties hebben grote kennis van de netwerk- en informatiesystemen van aanbieders in hun doelgroepen en de informatiebehoefte van die doelgroep.

Er zijn vier organisaties die krachtens de Wbni bij ministeriele regeling zijn aangewezen als computercrisisteam. Deze computercrisisteams zijn opgericht ten behoeve van sectoren om andere aanbieders daarbinnen bijstand te verlenen bij dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. Een voorbeeld van een computercrisisteam is de Stichting Z-CERT voor zorginstellingen. Naast genoemde computercrisisteams zijn er andere schakelorganisaties, die ten behoeve van aanbieders in verschillende regio's en sectoren in het leven zijn geroepen, die ook tot taak hebben om andere aanbieders binnen die sectoren te informeren en adviseren over digitale dreigingen en incidenten, en die inmiddels krachtens de Wbni als OKTT zijn aangewezen. Vanuit de verschillende departementen worden sectoren gestimuleerd om ook een schakelorganisatie ten behoeve van hun sector in het leven te roepen. Het NCSC heeft ook een handreiking gepubliceerd om zelf een samenwerkingsverband op te richten.

Overlap tussen de doelgroepen van schakelorganisaties, die krachtens de Wbni als computercrisisteam of OKTT zijn aangewezen, kan niet volledig voorkomen worden. Het is echter primair van belang dat andere aanbieders de voor hen relevante informatie ontvangen. Gelet daarop is het minder bezwaarlijk dat een andere aanbieder mogelijk, na verstrekking hiervan door het NCSC aan schakelorganisaties, dubbel informatie ontvangt over concrete dreigingen en incidenten dan dat deze aanbieders de informatie helemaal niet ontvangt.

De hiervoor bedoelde al bestaande schakelorganisaties maken ook deel uit van het Landelijk Dekkend Stelsel van cybersecuritysamenwerkingsverbanden (LDS). De overheid voert regie op de ontwikkeling van dit stelsel. In het kader van de Nederlandse Cybersecurity Strategie (NLCS) is het voornemen om het stelsel verder door te ontwikkelen en het zo efficiënt en effectief mogelijk in te richten, dit met als doel om versnippering en overlap zo veel mogelijk te voorkomen.

Is de AVG, volgens de regering, van toepassing op het verstrekken van persoonsgegevens door OKTT's?

Op de verwerking van persoonsgegevens door OKTT's, na de ontvangst daarvan van het NCSC, is inderdaad de AVG van toepassing.

De leden van de Volt-fractie merken op dat voor zover herleidbare gegevens over aanbieders met OKTT's worden gedeeld kan hier ook sprake zijn van persoonsgegevens, waaronder persoonsgegevens betreffende strafbare feiten als bedoeld in art. 10 AVG. Welke aanvullende maatregelen treft de regering om het verwerken van deze gegevens toe te staan, nu de verwerking ervan in beginsel verboden is?

Uit jurisprudentie van de Hoge Raad[1] volgt dat voor de vraag of persoonsgegevens strafrechtelijke persoonsgegevens in de zin van artikel 10 van de AVG betreffen, van belang is of sprake is van zodanige concrete feiten en omstandigheden dat zij een als een als strafbaar feit te kwalificeren bewezenverklaring – in de zin van artikel 350 Wetboek van Strafvordering – kunnen dragen. Hieruit volgt de maatstaf of vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan. Daarnaast speelt attributie – de mate waarin een strafbaar feit daadwerkelijk aan een persoon kan worden toegerekend – een rol in de vraag of een persoonsgegeven kan worden gekwalificeerd als strafrechtelijk persoonsgegeven.

De verstrekking van dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, door het NCSC aan of ten behoeve van andere aanbieders heeft tot doel om hen in de gelegenheid te brengen om maatregelen te nemen om digitale incidenten te voorkomen of te verhelpen en daarmee de digitale weerbaarheid van die aanbieders te vergroten. Deze verstrekking heeft niet tot doel om bijvoorbeeld handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. Ten aanzien van de enkele verwerking van een persoonsgegeven met het oog op het hiervoor genoemde doel geldt dat niet kan worden afgeleid dat sprake is van een gedraging die een zwaardere verdenking dan een redelijk vermoeden van schuld oplevert. Om te constateren dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld zullen naast een enkel persoonsgegeven namelijk meer concrete feiten en omstandigheden nodig zijn. Bovendien zal het te verwerken persoonsgegeven alleen in combinatie met andere

[1] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720.

tot een persoon herleidbare gegevens kunnen leiden tot attributie. Aan de bovengenoemde twee criteria (vaststellen dat sprake is van zodanige concrete feiten en omstandigheden dat zij op zich zelf genomen als een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren én aan een persoon kunnen toerekenen van een strafbaar feit) wordt aldus niet voldaan. De door het NCSC te verstrekken persoonsgegeven kunnen dus niet worden gekwalificeerd als persoonsgegevens betreffende strafbare feiten als bedoeld in artikel 10 van de AVG.

Hoe wordt bijvoorbeeld omgegaan met restdata en bijvangst en wie is daarvoor de verwerkingsverantwoordelijke? Kan de regering een lijst geven van de schakelorganisaties, OKTT's, computercrisisteams en andere aanbieders die vallen onder artikel 3, tweede lid a t/m e? Hoe wordt bepaald welke organisaties hier tot toe mogen treden? Wat is het toetsingskader aan de hand waarvan organisaties kunnen worden toegevoegd aan de lijst?

Artikel 3, tweede lid, Wbni regelt de bevoegdheid voor het NCSC om dreigings- en incidentinformatie, die relevant is voor andere aanbieders te verstrekken aan de in dit artikellid genoemde organisaties. Zoals ook toegelicht in de memorie van toelichting betreft het hierbij telkens dreigings- en incidentinformatie die is verkregen bij het verrichten van analyses ten behoeve van de primaire taak van het NCSC (bijstand aan vitale aanbieders en rijksoverheidsorganisaties). Mede gelet op artikel 17, eerste lid, Wbni is de Minister van Justitie en Veiligheid verwerkingsverantwoordelijke voor zover het gaat om het verstrekken van genoemde informatie, waaronder persoonsgegevens, aan bijvoorbeeld OKTT's. Vanaf het moment van ontvangst van deze informatie is het de ontvangende (schakel)organisatie die verantwoordelijk is voor het verwerken van die informatie in het kader van de taakuitoefening van die organisatie.

In reactie op het door deze leden gevraagde overzicht van de in artikel 3, tweede lid, Wbni bedoelde organisaties kan ik u mededelen dat bij ministeriële regeling (Regeling aanwijzing computercrisisteams) zijn aangewezen als computercrisisteams:
- de Informatiebeveiligingsdienst, onderdeel van VNG Realisatie B.V.;
- de Stichting Z-CERT;
- SURFcert, onderdeel van SURFnet B.V. en;
- CERT Watermanagement, onderdeel van het openbaar lichaam Het Waterschapshuis.

Bij ministeriële aanwijzing zijn aangewezen als OKTT's:
- Digital Trust Center;
- Vereniging Abuse Information Exchange;
- Stichting Nationale Beheersorganisatie Internetproviders (NBIP);
- Stichting Cyber Weerbaarheidscentrum Brainport (CWB);
- Cyberveilig Nederland;
- Connect2Trust en;
- FERM.

Onder de in dit artikel genoemde CSIRT's worden de door de lidstaten van de EU met inachtneming van artikel 9 van de NIB-richtlijn aangewezen CSIRT's verstaan; dat betreft dus ook het CSIRT voor digitale diensten, bedoeld in artikel 1 Wbni. Voor een nadere toelichting op welke aanbieders het betreft in het nieuw toegevoegde onderdeel e («andere aanbieders») verwijs ik graag naar het antwoord hierboven op onder meer eerdere vragen hierover van de leden van de Volt-fractie. Zoals hierboven in antwoord op de eerste vraag van de leden van de PVV-fractie is toegelicht vindt voorafgaand aan de aanwijzing van bijvoorbeeld OKTT's een grondige beoordeling plaats om te bepalen of verstrekking van

informatie aan die (schakel)organisatie op grond van artikel 3, tweede lid, Wbni verantwoord en gerechtvaardigd is. Graag verwijs ik voor een nadere toelichting op die beoordeling en de daarbij gehanteerde toetsingscriteria naar dat eerdergenoemde antwoord.

De regering geeft in de memorie van toelichting aan dat zowel publieke als private organisaties, zoals bedoeld in het voorgestelde artikel 3, tweede lid, onder e, zelf verantwoordelijk zijn voor het bepalen van de basis waarop zij die informatie verder verwerken. Vertrouwt de regering erop dat de juiste waarborgen in acht worden genomen door deze organisaties om de rechtmatigheid en veiligheid van de verdere verwerking te garanderen? Hoe kan dat worden gecontroleerd?

Een aanbieder is na de ontvangst van gegevens van het NCSC verwerkingsverantwoordelijke. Voor het treffen van maatregelen om digitale incidenten te voorkomen of om de gevolgen daarvan te beperken, kan het voor de aanbieder juist nodig zijn om ook de van het NCSC ontvangen persoonsgegevens te verwerken. Het is aan de aanbieder om als verwerkingsverantwoordelijke te beoordelen welke krachtens de AVG vereiste grondslag daarvoor kan worden aangewezen. Dit kan bijvoorbeeld gaan om het gerechtvaardigd belang als bedoeld in artikel 6, eerste lid, onderdeel f, van de AVG of het vervullen van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen als bedoeld in artikel 6, eerste lid, onderdeel e, van de AVG. De AP houdt het toezicht op de naleving van de AVG.

4. Verhouding NCSC – Digital Trust Center (DTC)

De leden van de VVD-fractie zouden graag willen weten hoe de «andere aanbieders» worden geïnformeerd over deze wetswijziging. Kan er met deze wetswijziging onduidelijkheid ontstaan voor «andere aanbieders» over waar ze terecht moeten wanneer er een cyberdreiging is? Zo ja, hoe wordt dit opgelost? Zo nee, waarom niet? Deze leden vragen daarnaast of deze wetswijziging juist niet een mooi moment kan zijn om het NCSC en DTC nog beter en intensiever samen te laten werken. Zo ja, op welke manier gaat dit ingevuld worden? Zo nee, waarom niet?

Andere aanbieders zullen middels een persbericht op de hoogte worden gesteld van deze wetswijziging. Naar mijn oordeel zal er voor andere aanbieders met dit wetsvoorstel geen onduidelijkheid ontstaan over waar zij terecht kunnen voor informatie over hen aangaande digitale dreigingen en incidenten. Voor zover andere aanbieders zijn aangesloten bij een schakelorganisatie weten zij uiteraard dat zij zich bij die organisatie voor die informatie kunnen vervoegen. Met het bij ministeriële regeling krachtens de Wbni aanwijzen van zowel computercrisisteams als OKTT's wordt bovendien verder verduidelijkt of hun schakelorganisatie ook als zodanig is aangewezen. Voor het niet-vitale bedrijfsleven is er voorts het DTC als schakelorganisatie. Daarnaast zijn er andere aanbieders die nog geen eigen schakelorganisatie hebben. Voorbeelden van zulke aanbieders zijn onder meer provincies, veiligheidsregio's en politieke partijen. Deze andere aanbieders zijn zelf primair verantwoordelijk om voldoende beveiligingsmaatregelen met betrekking tot hun netwerk- en informatiesystemen te treffen, om digitale incidenten te voorkomen of de gevolgen daarvan te beperken. Daarbij is het echter wel van belang dat ook zij over de nodige informatie over digitale dreigingen en incidenten komen te beschikken, zodat zij die maatregelen zo goed mogelijk kunnen nemen. Dit wetsvoorstel regelt daarom de bevoegdheid voor het NCSC om aan die aanbieders, in de gevallen waarin sprake is van een incident met (mogelijke) aanzienlijke gevolgen voor hun dienstverlening, daarover

rechtstreeks informatie te verstrekken. Daarnaast kunnen zij op grond van artikel 16 van de Wbni zelf bij het NCSC melding maken van dergelijke incidenten. Het staat andere aanbieders, die nog geen schakelorganisatie hebben, uiteraard ook vrij om met andere aanbieders een eigen schakelorganisatie in het leven te roepen, die het informeren over digitale dreigingen en incidenten van die aanbieders tot taak heeft én ook krachtens de Wbni als bijvoorbeeld OKTT zou kunnen worden aangewezen.

Zoals in de memorie van toelichting ook is aangegeven hebben het NCSC en het DTC duidelijk onderscheidenlijke primaire doelgroepen en taken. Het NCSC heeft primair het verlenen van bijstand (zoals het informeren) aan vitale aanbieders en rijksoverheidsorganisaties tot taak. Daarnaast heeft het tot taak om informatie betreffende andere aanbieders, die bij analyses ten behoeve van de primaire taak is verkregen, te verstrekken aan krachtens de Wbni aangewezen schakelorganisaties van die andere aanbieders (waaronder het DTC) en, in geval van inwerkingtreding van dit wetsvoorstel, dus mogelijk ook andere aanbieders zelf. Het DTC heeft tot taak om niet-vitale bedrijven te informeren en adviseren over digitale dreigingen en incidenten. Daarbij heeft het DTC onder meer tot taak om dreigings- en incidentinformatie die relevant is voor vitale aanbieders of rijksoverheidsorganisaties, indien het daarover beschikt, te verstrekken aan het NCSC. Met name ook door bovenbedoelde onderlinge verstrekking van informatie werken het NCSC en het DTC al samen om elkaar hierdoor in staat te stellen de onderscheidenlijke taken zo goed mogelijk uit te oefenen. Met de door de Minister van Economische Zaken en Klimaat voorgestelde Wet bevordering digitale weerbaarheid bedrijven, waarin genoemde taken van het DTC worden geregeld, wordt de afbakening van de taken van het NCSC en het DTC verder verduidelijkt.

Momenteel wordt bezien of en op welke manier het NCSC en het DTC verder kunnen samenwerken of wellicht zelfs kunnen integreren. De resultaten van deze verkenning worden deze zomer verwacht en zullen worden meegenomen in de Nederlandse Cybersecurity Strategie.

De leden van de PVV-fractie merken op dat het door de overlap in taakstelling tussen het NCSC en het DTC kan zijn dat er in tijden van crisis onduidelijkheden ontstaan omtrent de taken, bevoegdheden en/of rolverdeling van de organisaties. In de memorie van toelichting heeft de regering dit nader geprobeerd te concretiseren en wordt aangegeven dat de Wet bevordering digitale weerbaarheid bedrijven de taken van het DTC verder zal verduidelijken. Voor deze leden blijft het dan ook de vraag of, ook los van de Wet bevordering digitale weerbaarheid, de taken, bevoegdheden en/of rolverdeling van de respectievelijke organisaties met dit wetsvoorstel wel voldoende zijn geconcretiseerd en welke mogelijke aanpassingen van organisatorische aard de regering overweegt om een einde te maken aan de overlap in taakstelling.

De door de PVV-fractie gestelde overlap in taken en onduidelijkheden in taken, bevoegdheden en rolverdeling zie ik niet, zoals hierboven ook is toegelicht in antwoord op vragen van onder meer de leden van de SP-fractie. Het NCSC heeft krachtens de Wbni als primaire taak het informeren en het adviseren van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid over digitale dreigingen en incidenten. Naast het informeren en het adviseren verleent het NCSC de aanbieders in zijn doelgroep ook overige bijstand bij het treffen van maatregelen om incidenten te voorkomen en te verhelpen. Overige bijstand kan bijvoorbeeld inhouden dat aan de aanbieder uit de doelgroep ter plekke ondersteuning wordt geboden bij het duiden van het probleem en de maatregelen om dat probleem aan te pakken. Het DTC richt zich bij het

informeren en het adviseren over digitale dreigingen en incidenten op de doelgroep van het niet-vitale bedrijfsleven. Uitzondering op deze afbakening van doelgroepen zijn overigens digitaledienstverleners. Zij zijn geen vitale aanbieder, maar vallen ook niet in de doelgroep van het DTC. Zij vallen namelijk op grond van de Wbni onder het computer security incident response team (CSIRT) voor digitale diensten, dat hen bijstaat bij het treffen van maatregelen om de continuïteit van de dienst te waarborgen of te herstellen.[2] Door deze afbakening van doelgroepen en taken kan er geen verwarring ontstaan over van welke overheidsinstantie een aanbieder op bijstand kan rekenen bij digitale dreigingen en incidenten.

5. Verhouding tot hoger recht

5.1 Inleidende opmerkingen

De leden van de Volt-fractie merken op dat het concept van de NIB-richtlijn op 13 mei 2022 gereed was en nu ter beoordeling ligt. Het is aannemelijk dat hier weinig aan veranderd wordt, aangezien de BNC-fiches hier al in zijn verwerkt. Is het huidige wetsvoorstel van de Wbni voldoende voorbereid op de implementatie van deze richtlijn?

Over de herziening van de NIB-richtlijn is op 13 mei jl. een voorlopig politiek akkoord bereikt tussen de EU-lidstaten en het Europees Parlement. Naar verwachting wordt de richtlijn in het najaar van 2022 definitief vastgesteld, waarna deze moet worden geïmplementeerd in nationale wetgeving. Deze implementatie zal ook gevolgen hebben voor de Wbni, bijvoorbeeld vanwege de toename van het aantal aanbieders dat onder de toepasselijkheid daarvan zal komen te vallen. Vanwege de urgentie van deze wijziging is dit wetsvoorstel nu reeds in procedure gebracht. Overigens wordt hierbij opgemerkt dat nationale wetgeving (hetgeen dit wetsvoorstel betreft) niet kan worden gecombineerd met de implementatie van Europese regelgeving in nationale wetgeving.

5.2 EVRM

De leden van de Volt-fractie merken op dat de regering in de memorie van toelichting schrijft, ten aanzien van de dringende maatschappelijke behoefte, dat de samenleving in grote mate afhankelijk is van elektronische informatiesystemen, die onderling verweven zijn. Daarbij is het voorstelbaar dat het NCSC dreigingsinformatie moet delen, maar het gegeven – dat er grote afhankelijkheid bestaat – alleen, zegt nog niets over de maatschappelijke behoefte. Kan de regering aangeven in hoeverre er een concrete dreiging is die het NCSC noodzaakt om informatie te delen? Waaruit bestaat die dreiging precies? Of is het slechts een potentiële dreiging? Welke andere maatregelen kunnen eveneens getrokken worden om dreigingen te verminderen?

Met dit wetsvoorstel wordt het voor het NCSC in ruimere mate mogelijk om dreigings- en incidentinformatie, die relevant is voor andere aanbieders, al dan niet door tussenkomst van een schakelorganisatie, voor die aanbieders beschikbaar te maken. Zoals de leden van de Volt-fractie opmerken is in de memorie van toelichting, ter verklaring van de dringende maatschappelijke behoefte aan deze verruiming, inderdaad verwezen naar de grote afhankelijkheid van onder meer andere aanbieders van elektronische informatiesystemen ten behoeve van de uitoefening van diensten. Daarnaast is in diezelfde memorie van toelichting in dit verband echter ook gewezen op het feit dat er sprake is

[2] Zie artikel 4, vierde lid, van de Wbni.

van zowel een toename van het aantal (geslaagde) digitale aanvallen op andere aanbieders als een verzwaring van de impact van die aanvallen. Het is met het oog daarop niet wenselijk dat andere aanbieders verstoken blijven van informatie over digitale dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen, indien het NCSC daar wel over beschikt. Met die informatie kunnen deze aanbieders immers maatregelen treffen om incidenten te voorkomen of te verhelpen, zodoende de continuïteit van hun dienstverlening zo goed mogelijk te waarborgen, en daarmee nadelige maatschappelijke gevolgen zo veel mogelijk te voorkomen of te beperken. Voor verstrekking van informatie over dreigingen of incidenten aan andere aanbieders of hun schakelorganisaties geldt uiteraard dat die noodzakelijk moet zijn én dat het dus in elk geval steeds zal moeten gaan om informatie die voor de betrokken aanbieders in relatie tot hun netwerk- en informatiesystemen relevante dreigings- of incidentinformatie betreft. Van belang is hierbij ook dat het niet alleen zal kunnen gaan om informatie over aanvallen die al op aanbieders worden uitgevoerd, maar juist ook om informatie over dreigingen daarvan, zodat de betrokken aanbieders tijdig maatregelen kunnen nemen om zo te voorkomen dat aanvallen nadelige gevolgen kunnen hebben voor de continuïteit van hun dienstverlening. In de memorie van toelichting zijn enkele voorbeelden gegeven van aanvallen die zich in de afgelopen periode hebben voorgedaan. Zoals onder meer vermeld in het Cybersecuritybeeld Nederland zal in de aankomende periode onverminderd sprake zijn van een digitale dreiging en is het dus van groot belang dat ook andere aanbieders zo veel als mogelijk voor hen relevante informatie daarover van het NCSC ontvangen. Het is uiteraard primair de verantwoordelijkheid van aanbieders zelf om maatregelen te treffen om de beveiliging van hun systemen zo goed mogelijk op orde te hebben én daarmee te voorkomen dat dreigingen of incidenten nadelige gevolgen kunnen hebben voor de continuïteit van hun diensten of de gevolgen daarvan zo veel mogelijk te beperken. Daartoe is het echter wel van groot belang dat aanbieders zo veel als mogelijk, al dan niet door tussenkomst van een schakelorganisatie, de beschikking krijgen over informatie over hen aangaande digitale dreigingen en incidenten, zodat zij zo goed mogelijk in staat worden gesteld die maatregelen te treffen. Met dit wetsvoorstel wordt het mogelijk om de hierover bij het NCSC beschikbare informatie, in aanvulling op informatie die andere aanbieders uit andere bronnen kunnen verkrijgen, voor genoemde andere aanbieders in ruimere mate beschikbaar te maken.

In de memorie van toelichting schrijft de regering dat de voorgestelde nieuwe taak om persoonsgegevens aan andere aanbieders te verstrekken, gelet op de aard ervan, het doel en de overige waarborgen waarmee deze verwerking is omkleed, geen forse inmenging in het recht op respect voor iemands privéleven oplevert. Kan de regering dit nader toelichten? Welke waarde hecht zij aan de aard, het doel en de verschillende waarborgen? Met andere woorden, hoe worden deze factoren ingekleurd? Door het ontbreken van de toelichting daarop, kan deze conclusie niet worden gewaardeerd door deze leden.

De in artikel 3, tweede lid, onderdeel e, Wbni voorgestelde bevoegdheid voor het NCSC is dusdanig ingekaderd dat de verstrekking van (persoons-)gegevens alleen kan plaatsvinden aan de daarin bedoelde andere aanbieders, als er geen schakelorganisatie is die de aanbieder kan bedienen én de informatie ziet op een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder. De door wijziging van artikel 20, tweede lid, Wbni, voorgestelde bevoegdheid voor het NCSC om persoonsgegevens, die tevens vertrouwelijke tot aanbieders herleidbare gegevens zijn, te verstrekken aan OKTT's kan alleen worden gebruikt voor zover dat

dienstig is aan het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. De verstrekking van de genoemde gegevens geschiedt alleen voor zover dat noodzakelijk is voor het uitvoeren van de in artikel 3, tweede lid, Wbni genoemde taak. Dat betekent dus ook dat de genoemde (persoons)gegevens alleen met andere aanbieders of hun OKTT's worden gedeeld, indien die informatie relevant is voor de betrokken aanbieders en hen in staat stelt om zo nodig maatregelen te treffen om incidenten te voorkomen of de gevolgen ervan te beperken. Ten aanzien van de te verstrekken gegevens zal het met name gaan om IP-adressen, domeinnamen en e-mailadressen. Er worden geen bijzondere persoonsgegevens verstrekt. Dit maakt dat de inmenging in het recht op respect voor de persoonlijke levenssfeer geen forse inmenging betreft.

6. Toezicht en handhaving

Het verbaast de leden de GroenLinks-fractie dat er geen sprake zou zijn van toezicht op en handhaving van de naleving van verplichtingen. Worden hier geen gegevens uitgewisseld en verwerkt? Krijgen de OKTT's aanzienlijke bevoegdheden, zonder toezicht op de wijze waarop zij dit gaan uitvoeren?

Dit wetsvoorstel voorziet, net als de huidige wet, niet in toezicht op en handhaving van de naleving van verplichtingen door schakelorganisaties zoals OKTT's, omdat hiermee aan hen geen verplichtingen worden opgelegd. Evenmin creëert dit wetsvoorstel nieuwe bevoegdheden voor OKTT's. Dit voorstel regelt dat het NCSC in ruimere mate dreigings- en incidentinformatie over de systemen van de in dit voorstel bedoelde andere aanbieders aan de schakelorganisaties van deze andere aanbieders, meer in het bijzonder OKTT's, kan verstrekken, of direct aan deze andere aanbieders als een schakelorganisatie niet aanwezig is. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten. Dit wetsvoorstel zorgt ervoor dat OKTT's in meer gevallen dreigings- en incidentinformatie kunnen krijgen. Het is hun taak om, zodra zij deze informatie ontvangen van het NCSC, deze informatie te verstrekken aan de relevante aanbieders uit hun achterban. Als het gaat om de verwerking van persoonsgegevens na de ontvangst daarvan van het NCSC geldt dat OKTT's moeten voldoen aan de daaraan gestelde eisen op grond van de AVG. De AP ziet toe op de naleving van de AVG.

Deze leden lezen dat er bij aanwijzing als OKTT, de schakelorganisatie een verklaring ondertekent waarin is opgenomen dat aan het NCSC melding wordt gemaakt van onder meer belangrijke wijzigingen van de getroffen (technische en organisatorische) beveiligingsmaatregelen of van de doelgroep en de taken die ten behoeve van die doelgroep worden verricht. Acht de regering deze zelfrapportage voldoende op rechtmatige omgang met persoonsgegevens te garanderen?

Zoals hierboven in antwoord op de eerste vraag van de leden van de PVV-fractie is toegelicht vindt vóór aanwijzing van een organisatie als OKTT een grondige beoordeling plaats om te bepalen of het op grond van artikel 3, tweede lid, van de Wbni verstrekken van dreigings- of incidentinformatie verantwoord of gerechtvaardigd is. Ik verwijs voor een nadere toelichting op die beoordeling graag naar dat antwoord. Daarnaast is het inderdaad zo dat in geval van aanwijzing als OKTT de schakelorganisatie een verklaring ondertekent waarin is opgenomen dat melding aan het NCSC zal worden gemaakt van onder meer belangrijke wijzigingen van de getroffen beveiligingsmaatregelen of van de doelgroep en de taken die ten behoeve van die doelgroep worden verricht. Indien er op basis van

een dergelijke melding aanwijzingen zijn voor bijvoorbeeld een onvoldoende vertrouwelijke omgang door de OKTT met gegevens, dan kan verstrekking van gegevens door het NCSC worden opgeschort of kan de aanwijzing als OKTT zelfs worden ingetrokken. Het NCSC kan hiertoe echter ook overgaan als de onvoldoende vertrouwelijke omgang met gegevens blijkt uit andere bronnen. Van belang is voorts nadrukkelijk ook dat schakelorganisaties, als het gaat om de verwerking van persoonsgegevens, moeten voldoen aan de daaraan gestelde eisen op grond van de AVG, waaronder het kunnen aanwijzen van een grondslag voor rechtmatige verwerking, én dat op de naleving daarvan toezicht door de AP wordt gehouden. Naar mijn oordeel wordt hiermee, ook met inachtneming van de eigenstandige verantwoordelijkheid van schakelorganisaties voor de verwerking van persoonsgegevens, in voldoende mate gewaarborgd dat de verstrekking van informatie alleen geschiedt aan OKTT's die adequate maatregelen hebben getroffen voor onder meer een vertrouwelijke omgang met persoons- en andere gegevens die van die informatie deel uitmaken.

7. Advies en consultatie

7.1 Autoriteit Persoonsgegevens

De leden van de GroenLinks-fractie lezen dat de regering IP-adressen in dit verband niet ziet als persoonsgegevens betreffende strafbare feiten in de zin van artikel 10 AVG. Kan de regering nader motiveren waarom dit niet het geval zou zijn? Deze leden lezen dat het doel niet is om handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. Betekent dit dat er niet strafrechtelijk opgetreden gaat worden tegen deze partijen wanneer blijkt dat zij aanvallen plegen op de informatiehuishouding van «andere aanbieders»?

De voorgestelde gegevensverstrekking door het NCSC aan of ten behoeve van andere aanbieders heeft tot doel om hen in de gelegenheid te brengen om maatregelen te nemen om digitale incidenten te voorkomen of te verhelpen en daarmee de digitale weerbaarheid van die aanbieders te vergroten. Deze verstrekking heeft niet tot doel om handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. Dit wetsvoorstel regelt niet de strafrechtelijke vervolging van plegers van cyberaanvallen.

Ten aanzien van de enkele verwerking van IP-adressen met het oog op vorengenoemd doel geldt dat niet kan worden afgeleid dat sprake is van een gedraging die een zwaardere verdenking dan een redelijk vermoeden van schuld oplevert. Om te constateren dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld zullen naast IP-adressen namelijk meer concrete feiten en omstandigheden nodig zijn. Bovendien zullen de te verwerken IP-adressen alleen in combinatie met andere tot een persoon herleidbare gegevens kunnen leiden tot attributie. Aan de bovengenoemde twee criteria (vaststellen dat sprake is van zodanige concrete feiten en omstandigheden dat zij op zich zelf genomen als een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren én aan een persoon kunnen toerekenen van een strafbaar feit) wordt aldus niet voldaan. De IP-adressen dienen in dit verband derhalve niet als strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG te worden beschouwd. Ik verwijs hierbij tevens naar mijn antwoord hierboven op een vraag van de leden van de Volt-fractie over ditzelfde punt.

Daarnaast verbaast het deze leden dat de regering het advies van de Autoriteit Persoonsgegevens om met een betere afbakening van het begrip «andere aanbieders» te komen, afwijst. Dit vinden deze leden kwalijk. Het is van groot belang om expliciet en concreet te zijn in het geval van gegevensuitwisseling. Op dit moment, worden «andere aanbieders» voornamelijk gedefinieerd op kenmerken die zij niet hebben, zoals «niet een vitale aanbieder» of «een aanbieder die geen schakelorganisatie heeft». Kan de regering nader uitleggen waarom er gekozen is deze organisaties te definiëren met kenmerken die zij niet hebben, in plaats van kenmerken die zij wel hebben?

De regering is het uiteraard met de GroenLinks-fractie eens dat het bij gegevensverstrekking van belang is om expliciet en concreet te zijn over de groep waaraan kan worden verstrekt. Naar het oordeel van de regering is de in artikel 3, tweede lid, onderdeel e, Wbni voorgestelde bevoegdheid tot het verstrekken van dreigings- en incidentinformatie, waarop het advies van de AP betrekking had, voldoende concreet en expliciet omschreven. Bij deze bevoegdheid gaat het immers om de specifiek af te bakenen groep van aanbieders, die enerzijds geen vitale aanbieder en evenmin rijksoverheidsorganisatie zijn en daardoor buiten de in artikel 3, eerste lid, Wbni, bedoelde doelgroep vallen en anderzijds ook niet worden bediend door een andere schakelorganisatie. Door de bevoegdheid op de voorgestelde wijze vorm te geven en in te kaderen kan dreigings- en incidentinformatie worden verstrekt aan aanbieders die op dat specifieke moment niet tot de achterban van een schakelorganisatie behoren of als zo'n schakelorganisatie er niet meer is.

Ten aanzien van het benoemen van kenmerken die de in artikel 3, tweede lid, onderdeel e, bedoelde andere aanbieders wel hebben wordt het volgende opgemerkt. Deze groep van andere aanbieders betreft een diverse groep met uiteenlopende kenmerken. Het gaat bijvoorbeeld om politieke partijen, veiligheidsregio's en provincies. Door de diversiteit van aanbieders binnen deze groep is het vinden van algemene kenmerken (de gemene deler) die al deze organisaties hebben zeer gecompliceerd. Bovendien maakt het niet hebben van bepaalde kenmerken deze groep juist zo kenmerkend. Van de aanbieders uit deze groep is het immers kenmerkend dat zij allemaal niet vitale aanbieder of rijksoverheidsorganisaties zijn en ook niet worden bediend door een andere schakelorganisatie.

Het benoemen van de kenmerken die de in artikel 3, tweede lid, onderdeel e, bedoelde aanbieders wel zouden hebben leidt bovendien tot het risico dat er onverhoopt aanbieders buiten de groep vallen. Het is immers denkbaar dat een kenmerk niet wordt genoemd, simpelweg omdat een dergelijk kenmerk op dit moment niet in het vizier is. Dit leidt tot het risico dat deze aanbieders buiten de reikwijdte van de bevoegdheid vallen en daardoor geen dreigings- en incidentinformatie kunnen ontvangen over hun eigen netwerk- en informatiesystemen.

Deze leden zien ook dat de Autoriteit Persoonsgegevens adviseert aan te geven welke grondslag van verwerking van toepassing is op de verwerking door publieke aanbieders. De regering geeft aan dat de voorliggende wet de grondslag voor het delen van deze gegevens regelt en dat organisaties zelf verantwoordelijk zijn voor de grondslag waarop zij dat verwerken. Waarom is er gekozen om organisaties zelf verantwoordelijk te stellen voor het bepalen van de grondslag op basis waarvan zij informatie verwerken? Dreigt hierdoor niet een lappendeken aan wettelijke grondslagen? Vindt de regering dit wenselijk?

Een aanbieder is na de ontvangst van gegevens van het NCSC verwerkingsverantwoordelijke. Voor het treffen van maatregelen om digitale incidenten te voorkomen of om de gevolgen van digitale incidenten te verhelpen, kan het voor de aanbieder juist nodig zijn om ook de van het NCSC ontvangen persoonsgegevens te verwerken. Het is aan de aanbieder om als verwerkingsverantwoordelijke te beoordelen welke krachtens de AVG vereiste grondslag daarvoor kan worden aangewezen. Dit kan bijvoorbeeld gaan om het gerechtvaardigd belang als bedoeld in artikel 6, eerste lid, onderdeel f, van de AVG of het vervullen van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen als bedoeld in artikel 6, eerste lid, onderdeel e, van de AVG. De AP houdt toezicht op de naleving van ook dit vereiste in de AVG.

7.2 Cyber Security Raad (CSR)

De leden van de PVV-fractie hebben kennisgenomen van het advies van de Cyber Security Raad (CSR) die adviseert om meer helderheid te verschaffen richting bedrijven en maatschappelijke organisaties over wat zij van de verschillende partijen in het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden (LDS) kunnen verwachten. Daarbij heeft de CSR het advies herhaald om, in afwachting van de afwikkeling van de wijziging van de Wbni, nu al tot het delen van incidentinformatie met OKTT's over te gaan. De leden vragen of de regering van plan is om aan dit advies invulling te geven en hoe de regering dit gaat doen. Wat zijn de concrete plannen van de regering op dit punt?

Ik heb op 12 mei jl. een brief aan de Kamer gestuurd over het anticiperen op dit wetsvoorstel, waarin ik ook melding heb gemaakt van het door leden van de PVV-fractie genoemde advies van de CSR.[3] In deze brief heb ik aangegeven voor een dilemma te staan. Het dilemma ziet er enerzijds op dat zonder wettelijke grondslag niet mag worden overgegaan tot het delen van informatie. Anderzijds is er momenteel sprake van een reële digitale dreiging, die mogelijk grote gevolgen kan hebben voor de dienstverlening van de andere aanbieders en daarmee mogelijk grote impact kan hebben op de Nederlandse samenleving. Doordat het NCSC de hiervoor bedoelde informatie niet altijd kan delen, blijven veiligheidsrisico's in stand, met alle nadelige maatschappelijke gevolgen van dien. In deze brief bespreek ik daarom de mogelijkheid om in uitzonderlijke gevallen binnen de kaders van dit wetsvoorstel middels een vast afwegingskader toch over te gaan tot het in ruimere zin dan nu wettelijk mogelijk delen van informatie met andere aanbieders of hun schakelorganisaties. Het gaat hierbij enkel om gevallen van zwaarwegende redenen van maatschappelijke aard. Hierover is ook met uw Kamer gesproken tijdens het Commissiedebat van 25 mei jl.[4] Indien er naar mijn oordeel sprake is van een uitzonderlijk geval, dan zal uw Kamer hierover zoals afgesproken vertrouwelijk achteraf worden geïnformeerd.

7.3 OKTT's

De leden van de GroenLinks-fractie delen de zorg dat «bijzondere gevallen» een onvoldoende objectief en onvoldoende duidelijk criterium betreft. Het NCSC beoordeelt per geval of wordt voldaan aan de genoemde vereisten. Hoe garandeert de regering het voorkomen van willekeur bij deze beoordeling?

---

[3] Brief van de Minister van Justitie en Veiligheid van 12 mei 2022, Kamerstukken II 2021/22, 36 084, nr. 5.

[4] Verslag Commissiedebat Digitale Zaken 25 mei 2022, Kamerstukken II 2021/22, 36 084, nr. 7.

Zoals in de memorie van toelichting is toegelicht is de aanvankelijk in die memorie gebruikte term «bijzondere gevallen» onvoldoende duidelijk bevonden en daarom niet meer daarin gebruikt. Deze term wordt in het wetsvoorstel zelf niet gebruikt. Krachtens het daarin voorgestelde nieuwe onderdeel e van artikel 3, tweede lid, van de Wbni gelden er twee cumulatieve criteria waaraan vóór verstrekking van dreigings- of incidentinformatie door het NCSC aan andere aanbieders wordt getoetst alvorens tot verstrekking over te kunnen gaan. Deze voorwaarden zijn dat er geen schakelorganisatie is door tussenkomst waarvan die informatie aan de aanbieder kan worden verstrekt én dat er sprake is van informatie over een dreiging of incident met (mogelijke) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de aanbieder. Naar mijn oordeel zijn deze criteria voldoende objectief en duidelijk. Het klopt dat het NCSC per geval zal beoordelen of aan deze criteria wordt voldaan. Ik zie geen aanleiding om aan te nemen dat hierbij sprake zal kunnen zijn van willekeur. Aan de hand van de per geval beschikbare informatie over de aard en ernst van een dreiging en de (mogelijke) impact daarvan voor de dienstverlening van de specifieke aanbieder(s) zal telkens zorgvuldig worden beoordeeld of een dreiging of incident aanzienlijke gevolgen heeft of kan hebben.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius