36764 Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet)

36765 Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten)

Nr. 32 **VERSLAG VAN EEN WETGEVINGSOVERLEG**
Vastgesteld 28 mei 2026

De vaste commissie voor Justitie en Veiligheid en de vaste commissie voor Digitale Zaken hebben op 23 maart 2026 overleg gevoerd met de heer Van Weel, minister van Justitie en Veiligheid, over:

- het wetsvoorstel Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet) (Kamerstuk 36764);

- het wetsvoorstel Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten) (Kamerstuk 36765).

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

De voorzitter van de vaste commissie voor Justitie en Veiligheid,

Eerdmans

De voorzitter van de vaste commissie voor Digitale Zaken,
Dekker

De griffier van de vaste commissie voor Justitie en Veiligheid,
Van Tilburg

Voorzitter: Kathmann

Griffier: Paauwe

Aanwezig zijn acht leden der Kamer, te weten: Van den Berg, El Boujdaini, Emiel van Dijk, Faber, Kathmann, Martens-America, Vermeer en Zwinkels,

en de heer Van Weel, minister van Justitie en Veiligheid.

Aanvang 10.01 uur.

De **voorzitter**:

We gaan van start, want we hebben een drukke ochtend waarop we twee wetten bespreken: de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet. De heer Van den Berg, die naast mij zit, heeft superfancy boekjes, die hij nog uit gaat delen. Hij laat ze nu even zien. Voor straks bij de tweede termijn wil ik nog even de volgende bijsluiter geven. Omdat wij twee wetten in één keer bespreken, is het handig voor de griffie als u bij het indienen van moties even goed aangeeft bij welke wet de motie hoort.

Dat gezegd hebbende, beginnen we bij de heer Vermeer, want ik weet dat hij zich helaas rot rent van debat naar debat in dit gebouw. Hij moet helaas zo vertrekken, dus daarom geef ik als eerste graag het woord aan de heer Vermeer van de fractie van BBB. Uiteraard ook van harte welkom aan de minister.

De heer **Vermeer** (BBB):

Dank u wel, voorzitter. Heel hartelijk dank dat u mij toestaat aan de voorkant te spreken, zodat ik hier straks weer op een nette manier kan vertrekken.

Voorzitter. Eind april 2025 rond 14.00 uur 's middags werd het plotseling stil in twintig Nederlandse stadhuizen en provinciehuizen. Dat was niet omdat ambtenaren massaal aan de lunch zaten, maar omdat hun digitale voordeur met brute kracht werd ingeramd. Websites van gemeenten en provincies gingen plat door ddos-aanvallen van de pro-Russische hackersgroep NoName. Dit lijkt misschien een technisch incident, maar het is in werkelijkheid een politiek signaal, dat laat zien in welke wereld deze Cyberbeveiligingswet landt. Dat is een wereld waarin digitale ontwrichting geen uitzondering meer is, maar een dagelijks instrument in wat we inmiddels "hybride oorlogsvoering" noemen. We moeten daarover eerlijk zijn.

Cyberaanvallen zijn niet langer alleen het werk van criminelen die geld willen verdienen. Steeds vaker zijn het geopolitieke instrumenten, gericht op onze democratische instituties, onze economie en het vertrouwen van burgers in de overheid. Wanneer lokale overheden, die het dichtst bij de burger staan, doelwit worden, dan raakt dat ook direct het vertrouwen in onze publieke sector.

Voorzitter. Onze soevereiniteit in het digitale domein staat steeds vaker onder druk. Die constatering is niet overdreven, zeker nu de internationale verhoudingen veranderen en de geopolitieke rugdekking waarop Europa lange tijd kon rekenen, minder vanzelfsprekend lijkt. Dat betekent dat Nederland zijn eigen digitale weerbaarheid op orde moet hebben. We moeten onze digitale ophaalbruggen kunnen optrekken wanneer dat nodig is.

Voorzitter. In dat licht begrijpt BBB heel goed waarom deze Cyberbeveiligingswet er ligt. Met deze wet implementeren we de Europese cyberbeveiligingsregels uit de NIS2-richtlijn. Het doel is het verhogen van de digitale weerbaarheid van vitale en belangrijke organisaties. Dat onderschrijven we, maar tegelijkertijd zien we een patroon dat we vaker zien bij de implementatie van Europese regelgeving: Nederland wil weer het braafste jongetje van de klas zijn. Boven op de Europese verplichtingen worden nationale koppen gezet. Regels worden zwaarder, breder of ingewikkelder dan strikt noodzakelijk is. Dat roept vragen op, zeker omdat het Adviescollege toetsing regeldruk bij deze wet een kritisch en zelfs negatief advies heeft gegeven over de regeldruk. De vraag aan de staatssecretaris is dan ook simpel, of in dit geval aan de minister; sorry. Waarom kiest dit kabinet ervoor om dit ondanks dat negatieve advies toch door te zetten, zonder eerst de uitvoerbaarheid volledig inzichtelijk te maken?

Voorzitter. Vooral onze medeoverheden, provincies, gemeenten en waterschappen, maken zich grote zorgen. Zij zijn immers niet alleen uitvoerders van beleid; ze worden met deze wet zelf ook onder toezicht geplaatst. Organisaties zoals het Interprovinciaal Overleg en de Vereniging van Nederlandse Gemeenten waarschuwen al langere tijd dat de impact van deze wet zowel financieel als organisatorisch aanzienlijk zal zijn. Toch lezen wij in de stukken dat de kosten voor decentrale overheden nog in kaart moeten worden gebracht conform de Financiële-verhoudingswet. Dat baart mijn fractie zorgen. Daarom heb ik een aantal concrete vragen aan de minister. Waarom is er geen volledige Uitvoerbaarheidstoets Decentrale Overheden, een zogenaamde UDO, afgerond en gedeeld met de Kamer? Wanneer kan de Kamer die toets verwachten? Kan de minister toezeggen dat de wet pas volledig in werking treedt wanneer duidelijk is dat provincies en gemeenten de uitvoering daadwerkelijk aankunnen? Daarnaast speelt natuurlijk de financiële kant een rol, want we kennen allemaal het principe dat wie beleid maakt, ook betaalt voor de uitvoering, oftewel: knaken moeten taken volgen. Toch blijft het op dit punt stil. Is de minister bereid expliciet te garanderen dat provincies en gemeentes niet zelf voor de kosten van deze

nieuwe verplichtingen opdraaien? Komt er structurele financiering vanuit het Rijk voor de extra cyberbeveiligingstaken die deze wet oplegt? Kan hij inzicht geven in de orde van grootte van de kosten waar we hier over spreken?

Voorzitter. Dan de waterschappen. Voor de BBB zijn onze waterschappen een cruciale bestuurslaag. Zij zorgen er dagelijks voor dat Nederland droog blijft, dat we schoon drinkwater hebben en dat onze landbouw kan functioneren. In deze wet worden de waterschappen aangemerkt als essentiële entiteiten. Dat begrijpen wij, want drinkwater en waterveiligheid zijn vitale infrastructuur. Maar ook hier gaat het kabinet verder dan de Europese richtlijn. Ook het keren en beheren van waterkwantiteit wordt onder de wet gebracht, maar dat is niet verplicht volgens de Europese regels. Met andere woorden, opnieuw zien we een nationale kop. Daarom hebben wij de volgende vragen. Waarom kiest de regering ervoor om verder te gaan dan de Europese richtlijn voorschrijft? Welke concrete risicoanalyse rechtvaardigt deze uitbreiding? Heeft het kabinet de signalen van de waterschappen serieus genomen dat juist de uitvoeringslast van het Cyberbeveiligingsbesluit voor hen groot kan worden? Met andere woorden, voegen we hier daadwerkelijk veiligheid toe of vooral administratieve lasten?

Voorzitter. Een ander punt van zorg ligt in de voedselketen. Voor BBB is die uiteraard een essentieel onderwerp. De Wet weerbaarheid kritieke entiteiten, oftewel Wwke, is een mond vol iets wat in de kern heel simpel zou moeten zijn: hoe beschermen we de zaken die ons land draaiende houden? BBB vindt het dan ook een goede zaak dat de Wwke de sector productie, verwerking en distributie van levensmiddelen eindelijk bestempelt als kritiek en als een sector van maatschappelijk belang. Het is de erkenning waar BBB al jaren voor pleit, want zonder boeren, zonder voedselproductie, zonder transport staat Nederland stil. Een land dat zijn eigen voedselketen niet op orde heeft, is chanteerbaar en kwetsbaar. Die erkenning is terecht, maar erkenning alleen is niet genoeg. Wat hier dreigt, is een fundamentele tegenstrijdigheid in beleid. Wat hier gebeurt, is eigenlijk niet uit te leggen aan de mensen. Aan de ene kant bestempelen we de landbouw en voedselketen als kritiek, als onmisbaar voor onze nationale veiligheid en weerbaarheid, maar aan de andere kant stapelen we regels, verplichtingen en beperkingen op: stikstofbeleid, geluidsnormen, geurnormen, vergunningen die op slot zitten. Hierdoor krijgt juist diezelfde sector het steeds moeilijker om te blijven bestaan.

Voorzitter. Dat is geen consistent beleid, dat is beleid dat zichzelf tegenspreekt, bijvoorbeeld bij Mercosur. Hier zie je dat we de productie willen beschermen, maar we zetten wel de deur open voor producten tegen veel lagere standaarden uit Zuid-Amerika. Wat doet dit kabinet? Het zegt tegen onze boeren "jullie zijn cruciaal", maar tegelijkertijd maakt dit kabinet het ze bijna onmogelijk om hun werk nog te doen. Dan dringt zich de fundamentele vraag op of dit kabinet het nu echt meent als het zegt dat de voedselketen kritiek is. Of is het alleen een mooi label, terwijl het beleid in werkelijkheid gericht is op het steeds verder inperken en uit het land jagen van diezelfde

sector? Wat gaat het kabinet hieraan doen? Graag een reflectie van de minister hierop. Geen verwijzing naar ontijdigheid of andere ministers a.u.b. Immers, als iets echt van levensbelang is voor je land, ga je het beschermen, versterken en ondersteunen en niet uitknijpen met steeds nieuwe regels.

Voorzitter. BBB kiest duidelijk: wie cruciaal is voor Nederland, geef je ruimte. Juist daar wringt het. Als we kijken naar de praktijk, zien we iets anders gebeuren. De wet legt verantwoordelijkheden bij grote bedrijven, maar die schuiven hun verplichtingen weer door naar hun leveranciers. Wie zijn dat? Bijvoorbeeld bij voedselveiligheid en voedselzekerheid zijn dat de boeren, tuinders, transporteurs, mkb'ers. Dit zijn ondernemers die vaak niet eens onder deze wet vallen, maar wel geconfronteerd worden met eisen rond cyberveiligheid, certificering en rapportages. Het zijn eisen waarvoor zij niet de middelen, kennis of schaal hebben.

Voorzitter. We hebben het al eerder genoemd in diverse debatten, ook over rapportages rond duurzaamheid: er kan wel een uitzondering komen voor bedrijven onder de 250 medewerkers, maar zoals de ketenverantwoordelijkheid en ketensystemen werken, vallen mkb-bedrijven daar ook automatisch onder, want zij moeten juist de informatie aanleveren die grote bedrijven moeten … Uhm … Ik wou "factureren" zeggen, maar ik moet zeggen "rapporteren". Factureren doen ze zelf wel; daar maak ik mij geen zorgen over. Zo wordt weerbaarheid in de praktijk een papieren werkelijkheid, die vooral druk legt op de schouders van de kleinste schakels in de keten, en dat terwijl juist die schakels essentieel zijn. Zonder boer geen voedsel, zonder mkb geen keten en zonder keten geen zekerheid.

Voorzitter. Hoe voorkomt de minister dat grote ketenpartners hun verantwoordelijkheden simpelweg afwentelen op kleine ondernemers? Komt er duidelijkheid over wat wel en niet redelijk is om van leveranciers te eisen? Wordt, zoals het ATR, het Adviescollege toetsing regeldruk, adviseert, een volwaardige mkb-toets uitgevoerd, zodat de gevolgen voor kleine ondernemers vooraf inzichtelijk zijn? Als we de voedselketen echt als kritiek beschouwen, moeten we 'm ook beschermen, niet alleen tegen cyberdreigingen, maar vooral tegen beleid dat 'm van binnenuit onder druk zet.

Voorzitter. Dan het toezicht.

De **voorzitter**:

Voordat u naar het toezicht gaat, heeft u een interruptie van mevrouw Zwinkels van het CDA.

Mevrouw **Zwinkels** (CDA):

Ik begrijp het punt van de heer Vermeer als het gaat om het papierwerk dat druk kan leggen op het mkb, maar tegelijkertijd zie je in de waardeketens die de heer Vermeer beschrijft juist ook dat die kleinere bedrijven enorm kunnen meeliften op de cyberbeveiligingsmaatregelen van de grotere bedrijven, en dat ze elkaar zo kunnen versterken en daarop kunnen samenwerken. Deelt de heer Vermeer dat met mij en kunnen we het op die manier ook als een heel grote kans zien?

De heer **Vermeer** (BBB):

Ik zie dat nog totaal niet voor me, dus als mevrouw Zwinkels een voorbeeld zou willen noemen van hoe ze daarvan kunnen profiteren, dan hoor ik dat graag. Maar het is hier volgens mij niet de bedoeling om vragen terug te gaan stellen.

De **voorzitter**:

Nee, dat is niet de bedoeling. Maar het is wel aan mevrouw Zwinkels of zij nog een interruptie wil plaatsen. Zij heeft zo ook haar inbreng. Misschien komt zij er daarin op terug. Ik kijk even naar mevrouw Zwinkels of ze nog een interruptie heeft. Ja.

Mevrouw **Zwinkels** (CDA):

Ja, het kan kort. Ik denk dat er voldoende bedrijven zijn -- bij een paar ben ik ook op bezoek geweest -- waar dit aan de orde is, namelijk dat echt grote bedrijven hun leveranciers juist betrekken bij het beleid op cybersecurity. Ik hoop dat de heer Vermeer net als ik die kansen ziet. Voor de rest ga ik er in mijn eigen inbreng verder op in.

De heer **Vermeer** (BBB):

Ik denk zeker dat grote bedrijven kleinere bedrijven betrekken bij het beleid rond cybersecurity, maar dat betekent nog lang niet dat ze daarmee praktisch geholpen worden of dat überhaupt de kosten daarvoor gedeeld worden. Integendeel. Als er ook maar iets van een maatregel is die kostprijsverhogend werkt, dan is het over het algemeen zo -- dat hebben we ook gezien bij de bakkers met de energieprijzen -- dat men zegt "ja, maar dat is jullie bedrijfsaansprakelijkheid en jullie bedrijfsrisico; dat zijn jullie bedrijfskosten". Het klinkt dus mooier dan het is. Ik hoop dat mevrouw Zwinkels dit met fantastische voorbeelden gaat onderbouwen en dat wij dat ook in de praktijk gaan zien. Maar ik heb er vanuit mijn eigen ervaringen zware bedenkingen over hoe dat uiteindelijk uitpakt voor de kleinere bedrijven.

De **voorzitter**:

Meneer Vermeer, u kunt verder met uw betoog.

De heer **Vermeer** (BBB):

Voorzitter. Dan het toezicht. In verschillende sectoren zien we dat meerdere toezichthouders erbij betrokken raken. Een voorbeeld is de nucleaire sector, waar de Autoriteit Nucleaire Veiligheid en Stralingsbescherming al toezicht houdt, terwijl in dit wetsvoorstel ook de minister van Infrastructuur en Waterstaat een rol krijgt. Het kabinet zegt dat er samenwerkingsafspraken komen tussen de toezichthouders, maar eerlijk gezegd is dat nogal vaag en klopt het, denk ik, ook niet met de kaders en taken die zij toebedeeld gekregen hebben, omdat die duidelijk zijn over wat zij allemaal zelf moeten doen. Organisaties willen duidelijkheid. Zij willen weten waar ze aan toe zijn als er een incident plaatsvindt. Daarom de volgende vragen. Hoe wordt voorkomen dat organisaties met meerdere toezichthouders tegelijk te maken krijgen? Kan de minister garanderen dat één incident niet leidt tot meerdere onderzoeken en meerdere sancties? Is de minister bereid om, zoals het IPO voorstelt, een wettelijk verbod op dubbele boetes op te nemen? Dat zou een hoop onzekerheid wegnemen.

Voorzitter. Dan de evaluatie van deze wet. Volgens het wetsvoorstel wordt de wet pas na vijf jaar geëvalueerd. Op veel beleidsterreinen is dat een redelijke termijn, maar in de digitale wereld verandert alles razendsnel. Technologie ontwikkelt zich sneller dan wetgeving kan bijhouden. Daarom adviseert het ATR om al na één jaar een eerste evaluatie uit te voeren. Waarom wordt dit advies niet overgenomen? Is de minister bereid om in ieder geval een tussentijdse evaluatie na een of twee jaar te organiseren, zodat we tijdig kunnen bijsturen? Deze wet raakt naar schatting ruim 8.000 organisaties direct. Dan lijkt het BBB verstandig om eerder te luisteren naar de ervaringen uit de praktijk.

Voorzitter, ik rond af. De digitale luwte waarin Nederland lange tijd heeft geopereerd, bestaat niet meer. Cyberaanvallen worden agressiever, geopolitieke spanningen nemen toe en digitale infrastructuur is een strategisch doelwit geworden. Juist daarom is het belangrijk dat we onze digitale weerbaarheid versterken. Laten we er echter ook voor zorgen dat we een ophaalbrug bouwen die daadwerkelijk beschermt, en niet een constructie die zo zwaar is dat onze eigen medeoverheden en ondernemers eronder bezwijken.

Dank u wel.

De **voorzitter**:

Dank u wel voor uw bijdrage. U heeft een interruptie van de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):

Dank aan de heer Vermeer voor zijn bijdrage. Ik hoor best wel wat interessante punten terugkomen. Wij delen dezelfde zorgen op het gebied van toezicht op elkaar door de ANVS, zoals benoemd, maar ook wat betreft de evaluatietermijn en als laatste ook nog de dubbele boetes. Zou het in deze fase niet veel beter zijn om dat zelf als Kamer te amenderen, zodat we er zeker van zijn dat we zelf de regie kunnen pakken? Zoals u zegt, verandert de wereld namelijk inderdaad snel.

De heer **Vermeer** (BBB):

Als Kamer worden wij geacht kaders te stellen en te controleren. Ik heb liever dat de minister, vanuit de volle overtuiging dat dit goede ideeën zijn, zelf nog met een nota van wijziging komt, dan dat wij dat allemaal moeten gaan amenderen. Dat is niet omdat ik bang ben voor extra werk, want volgens mij liggen er al een aantal voorstellen van verschillende leden voor, maar omdat ik vind dat hier ook binnen de ministeries goed over moet worden nagedacht en dat men dit ook moet internaliseren. Dat werkt beter als men het zelf aanpast dan als wij een onderdeeltje eruit gaan amenderen.

De heer **Van den Berg** (JA21):

Daar ben ik het eigenlijk ook helemaal mee eens. Ik heb zelf de stukken doorgenomen en ik moet zeggen dat ik net als u wel verrast was dat die evaluatietermijn op vijf jaar staat. Ik ben eigenlijk wel nieuwsgierig hoe de heer Vermeer ernaar kijkt dat het ministerie tot zulke conclusies is gekomen. Ik blijf dat bijzonder vinden.

De heer **Vermeer** (BBB):

Ik denk dat ministeries hun tijd liever niet aan evaluaties besteden, zeker op korte termijn. Als zo'n wet doorgevoerd wordt, duurt het vaak vrij lang voordat je daarvan de effecten zou kunnen zien. Dat is in ieder geval het algemene idee. Als je nu al ziet wat voor reacties er allemaal op de wet zijn, zou ik zeggen: ga hem eerst eens even aanpassen. Daarnaast lijken evaluatietermijnen van twee of drie jaar veel redelijker, met name omdat dingen op het gebied van digitale zaken zo snel veranderen, zoals ik aangaf. Dan is een evaluatie op korte termijn het beste, al is het maar om de Kamer daarmee de kans te geven zich er even op te focussen en vervolgens ook

met wijzigingsvoorstellen te komen aan de hand van signalen uit sectoren of juridische procedures et cetera.

De **voorzitter**:

Het woord is aan de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):

Dank, voorzitter, minister en alle aanwezigen, fysiek en digitaal. Het is goed dat de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten vandaag op de agenda staan. Cyberbeveiliging en een weerbare maatschappij zijn tenslotte zeer belangrijk. Vandaag behandelen wij de implementatie van de Network and Information Security Directive 2, die eigenlijk al in 2024 geïmplementeerd had moeten worden. Het is duidelijk dat we deze termijn niet hebben gehaald. Hoewel deze wetten nauw met elkaar verbonden zijn, richten zij zich op verschillende terreinen en hebben zij een andere uitwerking. De Cyberbeveiligingswet richt zich voornamelijk op de digitale veiligheid en de Wet weerbaarheid kritieke entiteiten ziet op de fysieke weerbaarheid.

Als je beide wetten inhoudelijk bekijkt, wordt al snel duidelijk dat grove verschillen zichtbaar zijn. De Cyberbeveiligingswet noemt specifiek de CSIRT's, de Computer Security Incident Response Teams, voor bijstand bij incidenten. In de Wet weerbaarheid kritieke entiteiten wordt daarentegen geen specifiek fysiek Incident Response Team benoemd, maar ligt de nadruk op ondersteuning door de vakminister, terwijl de minister van Justitie en Veiligheid als centraal contactpunt de nationale en internationale coördinatie verzorgt. Ook wat betreft de meldplicht lijkt de Cyberbeveiligingswet strikter. Om aan de meldplicht te voldoen, wordt de melder geacht vier fasen te doorlopen, in tegenstelling tot de meldplicht in de Wet weerbaarheid kritieke entiteiten, die slechts bestaat uit twee fasen. Eveneens ontbreekt in de Wet weerbaarheid kritieke entiteiten de bestuurlijke trainingsverplichting in zijn geheel. Dit zijn pas enkele verschillen. Of de wetten dan ook gezamenlijk besproken hadden moeten worden, gezien de complexiteit, blijft de vraag.

Voorzitter. Nederland heeft belang bij heldere en goed werkende wetgeving. Deze twee wetten, die nu en in de toekomst van groot belang zullen zijn, moeten niet onderschat worden. Ondanks dat vele entiteiten duidelijkheid willen en behoefte hebben aan een snelle implementatie vinden wij dat implementatie pas verantwoord is zodra alle onduidelijkheden zijn weggenomen, zodat entiteiten daadwerkelijk weten waar zij aan toe zijn. Daarbij is het zo dat nog niet alle bedrijven zijn benoemd als belangrijke, essentiële of kritieke entiteit. Hoewel de entiteiten worden ondergebracht in een van de drie soorten entiteiten en de desbetreffende sector daarbij leidend is, zijn sommige entiteiten nog niet aangewezen. Als belangrijke of

essentiële diensten zijn bijvoorbeeld wel de drinkwatersector en de vervoersector aangewezen. Deze sectoren worden beschermd tegen ontwrichting. Als kritieke entiteiten zijn onder andere de gassector, elektriciteitssector en de oliesector aangewezen. Deze sectoren moeten beschermd worden tegen sabotage, natuurrampen en terroristische misdrijven. De wetten zijn al een aan aantal reparaties onderworpen geweest, laten we de wetgeving dan ook pas implementeren als deze echt gereed is.

Net zoals de minister de belangrijke zaken vaak in blokjes bespreekt, zal ik ook vandaag in blokjes de punten afgaan.

Voorzitter. Het eerste blokje betreft de bestuurlijke boete. Dit is mijn eerste punt. De minister geeft in de schriftelijke beantwoording aan dat de hoogte van de maximale boetes voortvloeit uit de NIS2-richtlijn en dat bij de toepassing daarvan het evenredigheidsbeginsel uit de Algemene wet bestuursrecht leidend is. Maar juist op dat punt blijft voor mijn fractie een belangrijke vraag liggen. Het gaat hier namelijk om zeer substantiële bedragen; boetes kunnen oplopen tot wel 7 à 10 miljoen euro of zelfs tot 2% van de omzet -- dus niet van de winst, maar van de omzet. Dat zijn bedragen die in absolute zin voor elke organisatie groot zijn, maar die in relatieve zin heel verschillend kunnen uitpakken. Ondanks het feit dat microbedrijven en kleine bedrijven buiten het toepassingsbereik van de Cyberbeveiligingswet vallen, blijft er bij JA21 zorg bestaan voor de middelgrote ondernemingen. Voor de mensen thuis: dit zijn dus entiteiten met 50-plus werknemers en bedrijven die jaarlijks meer dan 10 miljoen euro aan omzet genereren. Om het concreet te maken: een onderneming met een omzet van 100 miljoen euro wordt door een boete van bijvoorbeeld 7 miljoen euro relatief zwaarder geraakt dan een onderneming met een omzet van 500 miljoen euro. In dat laatste geval is de financiële impact beperkter in verhouding tot de schaal van de organisatie.

In tegenstelling tot de Cyberbeveiligingswet kan dit in de Wet weerbaarheid kritieke entiteiten ook kleinere kritieke entiteiten omvatten omdat het toepassingsbereik gebaseerd is op het belang van de entiteit voor de fysieke infrastructuur, ongeacht de omvang van de organisatie. Dat verschil in reikwijdte maakt het extra belangrijk om helder te hebben hoe de boetes en de handhavingspraktijk proportioneel en effectief worden toegepast.

Mevrouw **Faber** (PVV):

Ik heb even een verhelderende vraag. De heer Van den Berg heeft het over de verhoudingen tussen een groot en een klein bedrijf. Hij sprak over 500 miljoen omzet tegenover 100 miljoen omzet. Maar het gaat in feite toch om de winst, om wat je overhoudt? Je kunt een bedrijf hebben met 500 miljoen dat maar 1 miljoen winst heeft en je kunt een bedrijf hebben van 100 miljoen

dat 50 miljoen winst heeft. Dus volgens mij gaat de vergelijking enigszins mank.

De heer **Van den Berg** (JA21):

Ik snap dat punt van zorg, maar het gaat in deze wet alleen over een boete die is gebaseerd op de omzet en niet op de winst. Daar wordt dus inderdaad geen rekening mee gehouden. Om het te illustreren het volgende. Stel dat je een bedrijf hebt met een omzet van 100 miljoen euro. Dan val je dus onder die maximale tranche van 10 miljoen euro aan boete. Dat is dus 10%. Maar voor een bedrijf dat 500 miljoen euro groter is, valt onder de boete van 2%. Kortom, hoe groter je bent, hoe lager de relatieve zwaarte van de boete. Dat vinden wij een bezwaar.

Mevrouw **Faber** (PVV):

Ik vind toch dat u het winstaspect hierin niet meeneemt. Dat zou u juist wel mee moeten nemen, want hoeveel je overhoudt, heeft ook te maken met winst. Dat bepaalt hoe zwaar de boete is. Ik geef toe dat als de omzet hoger is, de boete lager kan zijn. Maar je moet het ook zien in relatie tot de winst.

De heer **Van den Berg** (JA21):

Zoals ik al zei, ben ik het daarmee eens. Ik heb daartoe een amendement in voorbereiding dat zegt dat je dat proportionele aspect moet afwegen bij het bedrijf: hoe staat het bedrijf ervoor en heeft het al eerder overtredingen begaan? Dan is het duidelijk wat het kader is. Ik denk dat winst daar wellicht een onderdeel van zou kunnen zijn, maar feit is hier wel dat bij een kleiner bedrijf de relatieve zwaarte van de boete in het meest ongunstige geval toch hoger kan uitvallen. Dat vinden wij eigenlijk een heel slecht signaal aan de markt. Daar moet je gewoon gelijk in zijn, of het nou gaat om een groot of klein bedrijf.

De **voorzitter**:

Meneer Van den Berg, u kunt verder met uw betoog.

De heer **Van den Berg** (JA21):

In omliggende landen -- denk aan Frankrijk, Estland, Duitsland en België -- waar het wetsvoorstel reeds is geïmplementeerd of zich nog in de implementatiefase bevindt, valt op dat dezelfde maxima worden gehanteerd, maar dat de praktische toepassing veel meer maatwerk kent dan vandaag bij

ons voorligt. Dat werd al even genoemd. Boetes worden aangepast aan de omvang en financiële draagkracht van de organisatie, er wordt gewerkt met omzetgerelateerde berekeningen of gefaseerde handhaving, en toezichthouders geven vaak eerst waarschuwingen of richten zich op het afdwingen van compliance voordat hoge boetes worden opgelegd, zodat kleine entiteiten niet disproportioneel zwaar worden getroffen. De minister geeft aan dat ook in Nederland in de praktijk vaak eerst met waarschuwingen wordt gewerkt. Dat is op zichzelf positief, maar het verschil lijkt te zijn dat het in andere landen meer structureel en expliciet is ingericht, terwijl het hier vooral als praktijk wordt beschreven.

Ik wil de minister daarom ook het volgende vragen. Hoe kijkt hij naar deze methode die andere landen hanteren? Ziet hij mogelijkheden om in Nederland een vergelijkbare praktijk te volgen om zowel middelgrote als kleinere entiteiten te beschermen? Mijn volgende vraag aan de minister is: hoe wordt in de praktijk voorkomen dat dit boetesysteem juist leidt tot een ongelijke uitwerking tussen kleine en grote entiteiten? De verwijzing naar het evenredigheidsbeginsel is op zichzelf belangrijk, maar dat blijft ook vrij abstract. Kan de minister daarom concreet toelichten op welke wijze bij het bepalen van de hoogte van een boete rekening wordt gehouden met de omvang en de draagkracht van een onderneming? Wordt daarbij bijvoorbeeld gekeken naar de omzet of andere financiële indicatoren zoals winst? Als dat niet structureel gebeurt, hoe voorkomt de minister dan dat kleine organisaties in de praktijk relatief zwaarder worden getroffen dan grotere spelers, terwijl het doel van deze wet juist is om de weerbaarheid in de gehele breedte te versterken? Graag een nadere, concrete toelichting op dit punt.

Voorzitter. Als tweede punt wil ik namens de fractie van JA21 graag ingaan op mogelijke groepsregistratie bij de meldplicht voor multinationals. Het gaat hierbij om grote organisaties die uit meerdere entiteiten bestaan, zoals moeder- en dochterondernemingen, waarbij de vraag is hoe de meld- en registratieplicht van de Cyberbeveiligingswet in de praktijk voor hen wordt vormgegeven. In een nota van toelichting op het Cyberbeveiligingsbesluit staat dat er wordt gewerkt aan een functionaliteit in het meld- en registratieportaal waarmee groepen van entiteiten meerdere entiteiten binnen een groep kunnen bundelen voor registraties en meldingen. Dat is een belangrijke stap. Kan de minister toelichten wanneer deze functionaliteit beschikbaar is en hoe precies wordt omgegaan met moeder- en dochterondernemingen? Hoe wordt voorkomen dat een entiteit die in meerdere sectoren actief is, dubbel of tegenstrijdig wordt geregistreerd of gemeld?

Voorzitter. Mijn derde punt: de samenloop tussen de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. Het uitgangspunt is dat alleen binnen de digitale sector de Cyberbeveiligingswet als lex specialis voorgaat. In andere gevallen kunnen entiteiten dus gewoon onder beide wetten vallen. Dat betekent dat niet alleen in de energiesector, maar ook in sectoren als

vervoer, drinkwater, gezondheidszorg en de productie, verwerking en distributie van de levensmiddelensector, organisaties met beide wetten te maken kunnen krijgen. Het kabinet geeft aan dat het doel is om administratieve lasten te beperken, onder andere door afstemming en informatie-uitwisseling tussen de bevoegde autoriteiten. Dat is het belangrijkste uitgangspunt. Maar daarbij wordt vooral gekeken naar de meld- en registratieplicht. Zo wordt duidelijk dat er één centraal meldpunt zal komen en de risicobeoordeling samengenomen mag worden. Wat echter onderbelicht blijft, is het risico op dubbel toezicht.

Dit beeld wordt bevestigd door de Autoriteit Persoonsgegevens, die aangeeft dat het huidige stelsel leidt tot inefficiënt toezicht. Waar sectorale toezichthouders slechts zicht hebben op hun eigen domein, beschikt de Autoriteit Persoonsgegevens over een breder, sectoroverstijgend beeld. Juist dat totaaloverzicht ontbreekt nu in de samenwerking, terwijl cyberbedreigingen zich niet beperken tot één sector. Daarnaast waarschuwt de Autoriteit Persoonsgegevens dat zonder goede afstemming, organisaties bij incidenten met meerdere toezichthouders te maken kunnen krijgen die vergelijkbare informatie opvragen, wat in crisissituaties dan weer zeer onwenselijk is.

De minister benadrukt dat het uitsluiten van volledige overlap niet mogelijk is. Wel hebben toezichthouders op grond van artikel 55 Cyberbeveiligingswet en artikel 25 Wet weerbaarheid kritieke entiteiten de verplichting om zo veel mogelijk samen te werken bij toezicht op de entiteiten. De heer Vermeer noemde dit net al. Tegelijkertijd blijft het formeel zo dat het toezicht vanuit beide wetten naast elkaar blijft bestaan, met eigen bevoegdheden en verantwoordelijkheden. Samenwerking en informatie-uitwisseling zijn natuurlijk belangrijk, maar bieden op zichzelf nog geen garantie dat dubbel toezicht in de praktijk wordt voorkomen.

Mijn vragen. Hoe wordt voorkomen dat een en dezelfde entiteit te maken krijgt met parallel toezicht door meerdere toezichthouders, ieder vanuit een eigen wettelijk kader? Betekent dit in de praktijk dat bedrijven alsnog met verschillende inspecties, beoordelingen en handhavingslijnen te maken kunnen krijgen? Kan de minister concreet toelichten hoe dit wordt gecoördineerd? Is er sprake van één leidende toezichthouder of blijft het bij samenwerking tussen meerdere autoriteiten? Hoe wordt geborgd dat dit voor bedrijven daadwerkelijk leidt tot minder lasten in plaats van een stapeling van toezicht? Kan de minister bovendien reflecteren op een alternatief waarbij de coördinatie sterker wordt geborgd, bijvoorbeeld door te werken met één leidende toezichthouder per entiteit, een soort van one audit-principe, of een meer geïntegreerde handhavingsaanpak?

Voorzitter. Ik zou graag willen ingaan op mijn vierde punt. Artikel 18 van het Cyberbeveiligingsbesluit gaat over een specifieke en vergaande bevoegdheid van de overheid in het kader van nationale veiligheid. Op grond van dit artikel kan een vakminister, in overeenstemming met de minister van Justitie

en Veiligheid, een entiteit verplichten om producten of diensten van bepaalde leveranciers te weren uit kritieke onderdelen van hun netwerk en informatiesystemen. Deze bevoegdheid kan worden ingezet wanneer er risico's zijn voor de nationale veiligheid, bijvoorbeeld als een leverancier mogelijk onder invloed staat van een staat die offensieve cyberactiviteit tegen Nederland ontplooit. Het gaat dus om situaties waarin de betrouwbaarheid van leveranciers direct raakt aan de veiligheid van vitale infrastructuur. Het is wel wonderlijk dat de artikelen van het Cyberbeveiligingsbesluit niet onder de relevante documenten zijn geschaard, maar dat dit document enige tijd geleden wel is verstuurd naar de Kamer en dat het Cyberbeveiligingsbesluit bovendien wel door de Raad van State wordt aangehaald.

Voorzitter. De minister heeft eerder duidelijk gemaakt dat artikel 18 van het Cyberbeveiligingsbesluit wordt gezien als een nadere uitwerking van de zorgplicht uit artikel 21 uit de Cyberbeveiligingswet, en dat het daarom op het niveau van een algemene maatregel van bestuur is geregeld. Tegelijkertijd roept dit bij de fractie van JA21 wel een fundamentele vraag op. De bevoegdheid om specifieke leveranciers te weren uit kritieke onderdelen van systemen is namelijk geen technische uitwerking, maar een zeer ingrijpende maatregel met grote gevolgen voor bedrijven. Kan de minister aangeven of dat besluit wel relevant is en of wij hier wel of niet over stemmen? En, zo ja, wanneer zullen wij hierover stemmen? Kan de minister toelichten waarom ervoor is gekozen om deze bevoegdheid niet op wetsniveau zelf te regelen, maar in lagere regelgeving?

Daarnaast blijft het punt van de totstandkoming knellen. Deze bepaling is pas in een laat stadium toegevoegd en heeft geen onderdeel uitgemaakt van de formele internetconsultatie. De minister geeft aan dat er wel gesprekken zijn gevoerd met koepelorganisaties, maar kan hij toelichten hoe breed en transparant deze consultatie is geweest en of alle relevante partijen daar bij betrokken zijn? Wat is de achterliggende reden van het feit dat deze bepaling later is toegevoegd?

Tot slot op dit punt -- niet getreurd, we zijn net over de helft -- hoor ik graag hoe de minister de rechtszekerheid voor bedrijven waarborgt. Op basis van welke concrete criteria wordt bepaald dat een leverancier een risico vormt en hoe voorspelbaar is dit voor bedrijven die afhankelijk zijn van dergelijke leveranciers en, niet te vergeten, onderaannemers?

Punt vijf, voorzitter. Naast de inhoudelijke bepalingen over boetes en zorgplicht wil ik namens JA21 ook ingaan op de evaluatie van de Cyberbeveiligingswet. Artikel 94 van het Cyberbeveiligingsbesluit legt nu vast dat de eerste formele evaluatie uiterlijk vijf jaar na inwerkingtreding plaatsvindt en daarna elke drie jaar. In de Wet weerbaarheid kritieke entiteiten is in artikel 41 een evaluatietermijn van vier jaar opgenomen, maar verder wordt er geen terugkerende evaluatietermijn genoemd.

Mijn fractie overweegt het artikel te amenderen op korte termijn, zodat er wel een terugkerende evaluatietermijn aanwezig is. De fractie van JA21 maakt zich zorgen over deze termijn, omdat digitale dreigingen en kwetsbaarheden in vitale sectoren snel kunnen veranderen. In een dreigingslandschap dat voortdurend evolueert kan een evaluatie van vijf of vier jaar betekenen dat cruciale knelpunten in de praktijk te lang onopgemerkt blijven. Dit geldt bijvoorbeeld voor de meldplicht, de zorgplicht en de toepassing van bestuurlijke boetes. Een termijn van maximaal twee jaar zorgt ervoor dat de wet tijdig kan worden bijgestuurd, wanneer blijkt dat onderdelen niet effectief zijn of niet praktisch uitvoerbaar zijn zonder dat er grote risico's voor entiteiten of de continuïteit van vitale processen ontstaan. Bovendien sluit een kortere evaluatietermijn beter aan bij het doel van de wet, namelijk het beschermen van vitale infrastructuur en het waarborgen van digitale veiligheid, terwijl bedrijven snel duidelijkheid krijgen over wat er van hen verwacht wordt.

De fractie van JA21 vindt een termijn van vier of vijf jaar voor de eerste evaluatie veel, maar dan ook veel te lang. Heel eerlijk: toen ik de wet voor het eerst las, kon ik niet geloven dat we voor zo'n lange termijn hebben gekozen. De wereld verandert snel, zeker op het gebied van digitalisering. We begrijpen de wens om aan te sluiten bij de evaluatiecyclus van de Europese Commissie, maar de risico's voor Nederlandse entiteiten, vooral in vitale sectoren, kunnen sneller veranderen dan de EU-cyclus aangeeft. Hoewel de minister aangeeft dat essentiële onderdelen via lagere regelgeving kunnen worden aangepast, geldt dat niet voor de kern van de wet, zoals de definitie van "essentiële entiteiten" of de zorg- en de meldplicht.

Het Adviescollege toetsing regeldruk heeft bovendien geadviseerd één jaar na de inwerkingtreding van zowel de Cyberbeveiligingswet als de Wet weerbaarheid kritieke entiteiten een invoeringstoets uit te voeren. Ook heeft het ATR aangegeven dat het kostenplaatje te rooskleurig en onvolledig is. Belangrijke kostenposten, zoals verplichte audits en inspecties, zijn nog niet volledig meegenomen. Daarom wijst het ATR op de eenmalige kennisnamekosten voor bedrijven, die oplopen tot circa 7,8 miljoen voor de ruim 8.000 betrokken organisaties.

Mevrouw **Zwinkels** (CDA):

Ik vind het punt van een kortere evaluatietermijn wel interessant. Tegelijkertijd denk ik ook wel dat het praktisch ondoenlijk is om elk jaar of elke twee jaar een hele uitgebreide evaluatie te doen en dan ook nog een keertje de wet te wijzigen. Als we bijna om het jaar de wet aanpassen en bedrijven weer moeten nadenken over waar ze nu weer aan moeten voldoen, dan zou dat namelijk ook heel veel regeldruk met zich meebrengen. Ik ben toch wel benieuwd of de heer Van den Berg het met mij eens is dat we in de wet een goede basis moeten neerzetten en we er tegelijkertijd in de praktijk

voor moeten zorgen dat we met elkaar alle ontwikkelingen bijhouden -- dat deel ik van harte met hem -- zodat we bedrijven daarop kunnen bijsturen of van informatie kunnen voorzien om daarop te reageren. Deelt hij dat met mij? Deelt hij, tot slot, ook met mij dat we de evaluatietermijnen van beide wetten misschien met elkaar gelijk moeten gaan trekken?

De heer **Van den Berg** (JA21):

Allereerst dank voor de kans om een slok water te nemen. Ik ben het wel met mevrouw Zwinkels eens dat je dat niet te frequent moet doen, maar feit is wel dat het Adviescollege toetsing regeldruk niet voor niets heeft geadviseerd eerst met zo'n invoeringstoets te beginnen. Dat is eigenlijk de eerste check, zo van: is dit nou goed gegaan en pakt de wet uit zoals we beoogd hebben? Daarna kan er natuurlijk een evaluatietermijn komen die terugkerend en langer is. Maar specifiek voor de Cyberbeveiligingswet: vijf jaar? Vijf jaar geleden hadden we nog niet eens ChatGPT en vijf jaar vanaf nu is er wellicht al kwantumtechnologie. In dat perspectief denk ik dat vijf jaar veel te lang is. In die zin zou een evaluatietermijn van twee jaar een eerste stap zijn. Als blijkt dat dat te frequent is, kunnen we dat altijd nog bij zo'n evaluatietermijn weer verlengen.

Ik ben het helemaal eens met het laatste punt van mevrouw Zwinkels over het synchroniseren van die termijnen. Juist omdat we het hier vandaag samen behandelen en die wetten ook zo veel samenhang hebben -- denk bijvoorbeeld aan die meld- en zorgplicht en aan het feit dat als je kritiek bent voor de ene wet, je essentieel bent voor de andere -- denk ik: er zit zo veel overlap in, dus synchroniseer dat inderdaad. Daar heb ik ook een amendement voor. Ik denk dat dit uiteindelijk ook goed zou zijn voor het wetgevingsproces hier omdat het sneller gaat en omdat het doel van de wet, namelijk weerbaarheid in de maatschappij, verder wordt ondersteund.

De **voorzitter**:

Meneer Van den Berg, u kunt verder met uw betoog.

De heer **Van den Berg** (JA21):

Nogmaals dank. Voor de overheid gaat het om een structureel bedrag dat oploopt tot circa 82,8 miljoen euro per jaar vanaf 2028, verdeeld over meerdere ministeries, voor onder andere toezicht, het centrale contactpunt en de versterking van de CSIRT's. Voor het bedrijfsleven wordt de structurele last van meldplicht geraamd op ongeveer €400.000 tot €450.000 per jaar -- dat is gebaseerd op zo'n 1.000 meldingen -- en een kostprijs van circa €432 per melding. Dat roept de vraag op of we hier wel een volledig beeld hebben van de werkelijke regeldruk. In het verlengde hiervan merken ook decentrale

overheden, zoals de waterschappen, op dat een grondige impactanalyse voorafgaand aan de inwerkingtreding ontbreekt. Juist bij wetgeving die zo veel verantwoordelijkheid bij decentrale partijen legt, is het essentieel om vooraf inzicht te hebben in uitvoerbaarheid, kosten en capaciteit. Het risico bestaat nu dat deze toets pas achteraf plaatsvindt, terwijl bijsturen dan complexer en bovendien ook kostbaarder is.

Hoe rechtvaardigt de minister het feit dat decentrale partijen verantwoordelijk worden gemaakt voor de uitvoering van deze wet, terwijl er vooraf geen volledig inzicht bestaat in de praktische en financiële gevolgen? Kan de minister verder toelichten of hij bereid is om de initiële evaluatieperiode te verkorten, bijvoorbeeld tot maximaal twee jaar, zodat Nederland sneller kan bijsturen als blijkt dat onderdelen van de wet in de praktijk niet goed werken? Hoe verhoudt zich dit tot de invoeringstoets die het ATR adviseerde? Kan de minister bovendien toelichten of hij bereid is om, mede in het licht van de invoeringstoets, expliciet te bezien hoe deze kosten, zowel voor de overheid als voor het bedrijfsleven, verder kunnen worden beperkt? En kan hij toezeggen dat er bij de invoeringstoets niet alleen wordt gekeken naar de werking van de wet, maar ook concreet naar de daadwerkelijke regeldruk in de praktijk, zodat waar nodig tijdig kan worden bijgestuurd? Kan de minister tot slot aangeven waarom er geen terugkerende evaluatietoets aanwezig is bij de Wet weerbaarheid kritieke entiteiten?

Voorzitter. Dan punt zes. Verder wil ik ingaan op de problematiek rondom de invulling van de zorgplicht. De invulling van de zorgplicht blijft ruim en vaag, waardoor het voor entiteiten lastig blijft om te bepalen of zij de zorgplicht op de juiste wijze hebben benaderd. Bedrijven moeten zelf inschatten wat proportioneel en effectief is voor hun specifieke risico's, waardoor praktische onzekerheid blijft bestaan. Zodra de Wet weerbaarheid kritieke entiteiten in werking treedt, hebben entiteiten immers tien maanden de tijd om die risicoanalyses uit te voeren. Partijen als FMO, VNO-NCW en de Unie van Waterschappen vroegen al om meer duidelijkheid bij het erkennen van bestaande normenkaders. Eveneens uitte de laatste instantie zorgen over het feit dat het zonder risicobeoordeling vanuit het ministerie onmogelijk is om een eigen risicoanalyse uit te voeren op grond van de Wet weerbaarheid kritieke entiteiten.

De minister heeft eerder aangegeven dat het voor bedrijven inderdaad lastig blijft om te bepalen welke maatregelen passend en evenredig zijn. Wel zegt de minister dat er verschillende maatregelen kunnen worden genomen met betrekking tot het uitvoeren van de desbetreffende zorgplicht. Zo zegt de minister dat de desbetreffende vakminister bijvoorbeeld ondersteuning kan bieden en dat er handreikingen opgesteld kunnen worden. Ook wordt momenteel een richtsnoer ontwikkeld door de Europese Commissie. Eveneens zal de toezichthouder per sector bepalen of de entiteit aan de zorgplicht heeft voldaan. Tot slot kunnen nadere regels eventueel via ministeriële regelingen worden vastgesteld. Men kan zich afvragen of dit niet thuishoort in formele wetten. De minister benadrukt dat de open norm

leidend blijft. Voor entiteiten blijven daarmee echter wezenlijke vragen onbeantwoord. Welke concrete eisen gelden ten aanzien van bijvoorbeeld firewalls? Welk niveau van monitoring wordt verwacht? En hoe verhouden nieuwe technologieën zoals kwantumencryptie zich tot deze open zorgplicht?

Voorzitter. Wat JA21 ook opvalt in de beantwoording, is dat er vaak wordt gesproken in termen als "kan", "kunnen" en "zal worden ontwikkeld". Dat wijst erop dat veel van de nadere invulling van de zorgplicht nog niet vastligt, maar invulling is van toekomstige uitwerkingen of beleidskeuzes, en dat de beoordeling daarvan kan verschillen per sector of toezichthouder. Het feit dat er momenteel nog geen concrete en eenduidige maatstaf bestaat, roept zorgen op bij mijn fractie. Kan de minister toelichten hoe wordt geborgd dat entiteiten op dit moment al voldoende duidelijkheid hebben over wat er concreet van hen wordt verwacht? Hoe wordt voorkomen dat hierdoor rechtsongelijkheid ontstaat tussen sectoren en dat bedrijven geconfronteerd worden met verschillende interpretaties van dezelfde zorgplicht? Kan de minister uitleggen hoe deze open norm zich verhoudt tot de mogelijkheid van hoge bestuurlijke boetes als voor bedrijven niet vooraf duidelijk is wanneer zij precies aan de norm voldoen? Kan de minister eveneens toelichten wanneer deze verschillende handvatten en duidelijke richtlijnen daadwerkelijk worden geboden in het kader van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten?

Voorzitter. Dan de Cariben -- een zonnige invalshoek. Mijn fractie wil ook graag stilstaan bij de positie van Caribisch Nederland. In het coalitieakkoord is juist benadrukt dat deze delen van Nederland beter betrokken moeten worden bij nationale wetgeving, zeker waar het gaat om veiligheid en weerbaarheid. Ook zou deze wet expliciet geldig zijn in het gehele Koninkrijk. Tegelijkertijd stelt de minister dat de Cyberbeveiligingswet en de implementatie van de NIS2-richtlijn op dit moment niet uitvoerbaar zijn voor Caribisch Nederland.

Dat roept bij mijn fractie enkele vragen op. Betekent dit dat vitale entiteiten in Caribisch Nederland voorlopig minder beschermd zijn tegen digitale dreigingen dan Europees Nederland? Daarnaast hoor ik graag van de minister wat er precies wordt bedoeld met "niet uitvoerbaar". Gaat het om capaciteit, om middelen of om wetgevingstechnische belemmeringen? Kan de minister een concreet tijdspad schetsen voor wanneer en op welke wijze Caribisch Nederland alsnog onder deze wetgeving zal vallen, zodat ook daar de digitale weerbaarheid op orde komt? Kan de minister verder toelichten of de mogelijkheid aanwezig is dat de implementatie van de wetten in Caribisch Nederland bijvoorbeeld kan plaatsvinden gezamenlijk met de eerste evaluatietermijn?

Voorzitter, nu echt tot slot. De Algemene verordening gegevensbescherming, de AVG, is ook van belang voor de verwerking van persoonsgegevens onder de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet. Het verwerken van persoonsgegevens is een inmenging in het recht op de

persoonlijke levenssfeer, vastgelegd in artikel 8 van het EVRM -- ik had niet verwacht dat ik daar ooit aan zou refereren! Deze inmenging wordt gerechtvaardigd omdat deze bij wet is voorzien en noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid en het economisch welzijn. Zonder deze gegevens kunnen instanties zoals het CSIRT immers geen bijstand verlenen of waarschuwingen sturen naar de juiste personen binnen een organisatie.

De bewaartermijn van 60 maanden tot 10 jaar voor bijzondere persoonsgegevens onder de Cyberbeveiligingswet wordt echter als erg lang ervaren. Zo merkte de Autoriteit Persoonsgegevens op dat de bewaartermijn van 60 maanden steeds opnieuw zou gaan lopen bij elke wijziging in het register. Omdat bedrijven hun gegevens actueel moeten houden, zouden deze persoonsgegevens in de praktijk nooit worden verwijderd. De minister heeft naar aanleiding van dit advies de tekst aangepast. In plaats van na de laatste wijziging begint de termijn nu te lopen vanaf de laatste bevestiging van juistheid.

De minister stelt dat het niet wenselijk is om gegevens te verwijderen die nog steeds relevant zijn voor wettelijke taken, maar benadrukt dat gegevens nooit langer mogen worden bewaard dan strikt noodzakelijk. Voor de zeer bijzondere persoonsgegevens is de bewaartermijn voor het CSIRT aanzienlijk verkort, van 60 maanden naar 12 maanden. Voor toezichthouders wordt echter uitgegaan van een bewaartermijn van 60 maanden, in verband met de noodzaak van dossieropbouw, langdurige juridische procedures en de uitvoerbaarheid van toezicht. Voor reguliere persoonsgegevens geldt zowel bij de Wet weerbaarheid kritieke entiteiten als de Cyberbeveiligingswet een bewaartermijn van maximaal 120 maanden voor toezichthouders. Voor overige wettelijke taken geldt een maximale bewaartermijn van 60 maanden.

Voorzitter. Een maximale termijn van tien jaar lijkt disproportioneel lang. De minister benadrukt dat een dergelijke termijn noodzakelijk is voor onder andere de opbouw van het dossier en eventuele bestuursrechtelijke procedures. Tegelijkertijd gaat het hier om een zeer lange bewaartermijn voor reguliere persoonsgegevens. Dit onderwerp is eveneens door verschillende partijen en instanties nadrukkelijk ter discussie gesteld, en terecht. Zo hebben de G4-gemeenten hun zorgen geuit over de termijn van 60 maanden voor loggegevens, onder meer vanwege de kosten en de uitvoerbaarheid. Mijn fractie vraagt zich af hoe deze termijn zich verhoudt tot het proportionaliteitsbeginsel onder de AVG en artikel 8 van het EVRM. Kan de minister nader onderbouwen waarom een kortere bewaartermijn niet volstaat? Denk bijvoorbeeld aan twaalf maanden, zoals bij andere taken binnen dezelfde wet.

Daarnaast hoor ik graag hoe wordt geborgd dat de maximale termijn in de praktijk niet standaard wordt, maar dat daadwerkelijk per dossier wordt beoordeeld of eerder verwijderen mogelijk is. Kan de minister bovendien toelichten hoe de termijn van 60 maanden zich precies verhoudt tot het

noodzakelijkheidscriterium in de praktijk? In hoeverre wordt per dossier daadwerkelijk beoordeeld of een kortere bewaartermijn mogelijk is? Of fungeert deze termijn in de praktijk als de standaard?

Daarnaast blijft voor mijn fractie de vraag bestaan waarom het verschil met het CSIRT zo groot is. Als het CSIRT kan volstaan met 12 maanden voor bijzondere persoonsgegevens, kan de minister dan nader onderbouwen waarom voor toezichthoudende taken een termijn van 60 maanden noodzakelijk is? Zijn er mogelijkheden om hier tot verdere verkorting of differentiatie te komen?

Voorzitter, dat was het dan. Dank u wel.

De **voorzitter**:

Van harte dank voor uw bijdrage, meneer Van den Berg. Het woord is aan mevrouw Faber van de PVV.

Mevrouw **Faber** (PVV):

Dank u wel, voorzitter. Ik zal het alleen over de Wet weerbaarheid kritieke entiteiten hebben. Het andere gedeelte doet mijn collega, meneer Van Dijk.

Voorzitter. Om onze democratische rechtsstaat overeind te houden, is het van belang dat wij vitale processen die gevoelig kunnen zijn voor onder andere terroristische aanslagen, beschermen. Stelt u zich eens voor dat de stroom langdurig uitvalt; dat heeft niet alleen consequenties voor het huiselijk comfort, maar ook de criminaliteit zal sterk toenemen. Het voorliggende wetsvoorstel ter implementatie van de CER-richtlijn heeft als doel om essentiële diensten, ook wel "kritieke entiteiten" genoemd, veilig te stellen. U kunt hierbij denken aan de eerste levensbehoefte, namelijk water. Het is van levensbelang dat de drinkwaterbedrijven blijven functioneren. Door dit wetsvoorstel krijgen zij en alle andere bedrijven met essentiële diensten verplichtingen, zoals het maken van een risicobeoordeling om alle relevante door de natuur en de mens veroorzaakte risico's in kaart te brengen. Daarnaast hebben ze een zorgplicht om de weerbaarheid te vergroten en een meldplicht bij een eventueel incident. Nederland kent op dit moment al een vergelijkbare methode door het staande beleid van de Aanpak vitaal. Dat beleid heeft veel raakvlakken met de CER-richtlijn en wordt door vitale aanbieders al beleidsmatig nagestreefd. Er is al veel samenwerking tussen departementen en door hen aangewezen vitale aanbieders om de weerbaarheid te versterken.

Voorzitter. Dikwijls klopt het allemaal wel op papier, maar kan de praktijk weerbarstiger zijn. Het is positief dat het wetsvoorstel voorziet in een zorgplicht die ook fysieke bescherming van gebouwen en infrastructuur behelst, onder andere door middel van omheiningen, detectieapparatuur en

toegangscontroles. De Franse opwerkingsfabriek La Hague wordt bewaakt door speciaal getrainde beveiligingsteams van de Franse overheid, zelfs afweergeschut ontbreekt niet. Hoever gaan de maatregelen die voortkomen uit dit wetsvoorstel voor bijvoorbeeld een Nederlandse kerncentrale? Wordt deze ook beschermd door bijvoorbeeld Defensie?

Het toezicht op de entiteiten ligt bij de vakministers. Zij zijn al de bevoegde autoriteit in hun sectoren. De minister van Justitie en Veiligheid heeft daarbovenop een coördinerende taak. De NCTV functioneert als centraal contactpunt. De minister kan een nationale kop plaatsen door meer sectoren aan te wijzen dan verplicht is vanuit de richtlijn. Hiermee drukt hij bedrijven in een ongelijk speelveld. Dat is ongewenst voor ons bedrijfsleven, dat toch al gebukt gaat onder verstikkende regelgeving en bijkomende kosten. De minister zou in het kader van de nationale veiligheid over deze bevoegdheid willen beschikken. Kan de minister dit nader duiden? De PVV houdt niet zo van nationale koppen. 80% van de vitale processen is in handen van private partijen die onder toezicht staan van de vakministers, onafhankelijk. De resterende 20% betreft vitale processen binnen de overheid. Die staan onder toezicht van de minister van Binnenlandse Zaken. Onafhankelijk, of toch niet? De overheid controleert in dezen de overheid. Het is een dingetje zoals: de slager keurt zijn eigen vlees. Hoe gaat de minister dit oplossen?

Er is nog zo'n gevalletje van toezicht, namelijk het zelfstandig bestuursorgaan, afgekort zbo. Een zbo voert zelfstandig taken uit zonder directe aansturing van een minister en neemt dan ook onafhankelijk beslissingen. Ik noem een voorbeeld. In de Kernenergiewet zijn toezicht- en handhavingsbevoegdheden uitdrukkelijk toegekend aan de Autoriteit Nucleaire Veiligheid en Stralingsbescherming, afgekort de ANVS. De reden dat de ANVS een zbo werd, was dat die onafhankelijkheid noodzakelijk was op grond van internationaal en Europees recht. Beslissingen van de ANVS moesten namelijk genomen kunnen worden zonder druk van belangen die kunnen conflicteren met het belang van veiligheid, zo meende de regering toen.

Voorzitter. Ik raak nu enigszins in verwarring. Aan de ene kant moesten zij zelfstandig kunnen besluiten in het belang van de veiligheid en aan de andere kant moet de minister nu het heft in handen kunnen nemen. Maar hoe gaan we dan bijvoorbeeld om met een incident in een kerncentrale? Nu ligt het toezicht op de veiligheid van de kerncentrale bij de ANVS. Bij het in werking treden van deze wet komt dit tevens te liggen bij de minister van IenW. Kan de echte toezichthouder zich in dezen melden? Graag een reactie van de minister.

Er kunnen meerdere toezichthouders tegelijk bevoegd zijn als er een zbo bij betrokken is of als meerdere vakministers betrokken zijn bij een entiteit die in meerdere sectoren voorkomt. Het risico bestaat dan dat vakministers de hete aardappel bij de ander op de financiële plaat leggen. Dit geldt vooral bij departementen met een krappe begroting. De minister heeft er dan namelijk

niet voor gekozen om de kritieke entiteit financieel te ondersteunen. De kosten daarvoor gaan af van de eigen begroting. Dit kan leiden tot een hoop getouwtrek met als gevolg dat geen van beiden toezicht houdt en handhaaft. Hoe gaat de minister dit oplossen?

Tot zover, voorzitter.

De **voorzitter**:

Dank u wel, mevrouw Faber. Er zijn geen interrupties. Dan is het woord aan mevrouw Martens-America van de VVD.

Mevrouw **Martens-America** (VVD):

Dank, voorzitter. De digitale wereld krijgt een steeds grotere rol in onze samenleving. Belangrijke sectoren zoals zorg, onderwijs, energiebedrijven en noem maar op, kunnen niet meer zonder een goedwerkende en veilige digitale infrastructuur. Geopolitieke spanningen en het feit dat onze overheid volledig afhankelijk is van digitale netwerken, maken het invoeren van deze wetten urgenter dan ooit. Ons land wordt dagelijks geconfronteerd met hybride dreigingen en aanvallen.

Voorzitter. Een cyberaanval kan veel schade aanrichten bij bedrijven en kan daarmee ook onze economie en samenleving als geheel raken. Soms blijven de onlinewereld en de digitale infrastructuur abstracte begrippen, maar we hebben recent nog gezien welke gevolgen een hack bij bijvoorbeeld het bedrijf Odido kan hebben voor onze maatschappij. Dit is een voorbeeld van een zichtbare situatie, maar het overgrote deel wordt tijdig tegengehouden of bereikt nooit het publieke oog.

Voorzitter. Mijn fractie hoopt dat Nederland en Europa met deze wetten de digitale en fysieke weerbaarheid van belangrijke sectoren tegen cyberaanvallen versterken. Wat de VVD betreft treden ze zo snel mogelijk in werking. Toch heb ik daarover mijn eerste vraag aan de minister. Waarom heeft de implementatie van deze twee wetten daadwerkelijk zo lang geduurd? Welke gevolgen heeft deze vertraging gehad voor onze cyberveiligheid en onze bedrijven? Hebben er zich in de tussentijd situaties voorgedaan die ons hebben laten inzien dat er al extra stappen nodig zouden moeten zijn boven op de bestaande wetten die we op dit moment bespreken? Ik wil in mijn bijdrage graag de volgende drie punten maken: duidelijkheid voor ondernemers, de evaluatieperiode en het inrichten van registratieloketten.

Mijn eerste punt is de duidelijkheid voor ondernemers. Het beschermen van onze bedrijven is ontzettend belangrijk en dat betekent dat we ook de wetgeving moeten aanpassen, processen anders moeten inrichten en, als het tegenzit, de regels voor ondernemers mogelijk complexer moeten maken.

Wat de VVD betreft is het vooral belangrijk dat het voor ondernemers helder is op welke manier zij met deze nieuwe extra handelingen kunnen bijdragen aan het grote collectief, namelijk de veiligheid van ons land. Het moet daadwerkelijk geen papieren tijger worden. Mijn vraag aan de minister is dan ook hoe we deze bedrijven en ondernemers meenemen in het belang hiervan. Dat is hier ook al eerder genoemd. Vooral de wat kleinere bedrijven gaan toch een wat zwaardere rol spelen in het grote geheel. Hoe maken we die bedrijven duidelijk dat ook zij essentieel zijn in deze uitdaging? Waar wordt bijvoorbeeld hun feedback op dit proces en op de implementatie van deze wetten daadwerkelijk verzameld? Hoe gaan we ervoor zorgen dat zij gehoord worden?

Daarnaast heb ik een vraag over de bedrijven die in meerdere sectoren actief zijn. Voor hen is het nu niet altijd duidelijk onder welke regels binnen de Cyberbeveiligingswet zij precies vallen. Kunnen de sectordefinities verduidelijkt worden, zodat ondernemers beter weten waar ze aan toe zijn? Tot slot op dit punt vraag ik hoe bestuurders worden geïnformeerd over al de te nemen stappen voor zowel de meldplicht, de zorgplicht en de registratieplicht. Hoe worden zij hierover geïnformeerd? Hoe voorkomt het kabinet dat bestuurders onnodig in de problemen komen, omdat zij per ongeluk een verplichting missen? Dat is mij niet helemaal duidelijk. Misschien kan de minister hier nog een toelichting op geven.

Dan kom ik op de evaluatieperiode. Daarover is al eerder een interruptiedebatje gegaan. Ik sluit me aan bij de zorgen van de heer Van den Berg dat de termijn van vijf jaar te lang is. De wetsvoorstellen worden namelijk na vijf jaar geëvalueerd. De minister heeft al eerder naar aanleiding van het advies van het ATR aangegeven dat een evaluatie na één jaar te vroeg zou zijn voor een zorgvuldige evaluatie. Ik wil de minister vragen hoe er toch eerder dan pas na vijf jaar een evaluatie zou kunnen worden uitgevoerd met de argumentatie die de heer Van den Berg hier al heeft aangevoerd, namelijk dat we worden ingehaald door de dagelijkse realiteit. Mijn fractie voelt veel voor een evaluatietermijn van twee jaar.

Dan het inrichten van het registratieloket. Zoals ik al eerder heb aangegeven, wil ik benadrukken dat deze wetten er toch wel echt snel moeten komen. Het moment lijkt nu dan toch eindelijk daar. Er zal ook zorgvuldig moeten worden gekeken naar het inrichten van bijvoorbeeld het registratieloket voor ondernemers. De registratieplicht verplicht organisaties om zich in te schrijven bij een nationaal register. Hier is echter nog veel onduidelijkheid over. Dat is ook de feedback die wij van veel bedrijven hebben ontvangen. Wat kan deze minister doen om informatie over dit loket dan ook zo snel mogelijk te delen met ondernemers, zodat ondernemers goed weten waar ze aan toe zijn en ze ook zo snel mogelijk de eerste stappen van de voorbereiding kunnen zetten?

Voorzitter. De VVD is blij met de wetten. Het beveiligen van systemen is urgenter dan ooit en vraagt dan ook om goede wetgeving. Dank u wel.

De **voorzitter**:

Dank u wel voor uw bijdrage. Het woord is aan mevrouw Zwinkels van het CDA.

Mevrouw **Zwinkels** (CDA):

Dank u wel, voorzitter. Vandaag bespreken we twee wetsvoorstellen die nauw met elkaar samenhangen: de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet. Het eerste voorstel ziet vooral toe op de fysieke en organisatorische weerbaarheid van kritieke entiteiten en het tweede op de digitale weerbaarheid van essentiële en belangrijke entiteiten. Samen raken ze direct aan de bescherming van vitale processen en daarmee aan de weerbaarheid van onze samenleving.

Ik begin met de Wet weerbaarheid kritieke entiteiten. Met deze wet wordt de Europese CER-richtlijn geïmplementeerd. Daarmee wordt een minimumniveau geïntroduceerd voor de weerbaarheid van essentiële diensten in een aantal vitale sectoren tegen risico's en bedreigingen. Het gaat daarbij om diensten die van cruciaal belang zijn voor het functioneren van onze maatschappij, economie, volksgezondheid, openbare veiligheid en milieu. Uitval van deze diensten kan verstrekkende en ontwrichtende gevolgen hebben, niet alleen nationaal, maar ook voor de Europese Unie. Dat zijn dus niet zomáár sectoren. Het zijn sectoren die onze samenleving draaiende en veilig houden. Juist daarom is het van groot belang dat hun weerbaarheid structureel wordt versterkt. Het CDA onderschrijft daarom ook het uitgangspunt van deze wet en het belang van de voorgestelde risicobeoordelingen.

Voorzitter. Op grond van de CER-richtlijn zijn lidstaten verplicht om een nationale risicobeoordeling op te stellen. Daarnaast moeten kritieke entiteiten zelf periodiek een risicobeoordeling uitvoeren. Kan de minister toelichten hoe deze beoordelingen zich tot elkaar verhouden? Hoe wordt voorkomen dat deze trajecten los van elkaar plaatsvinden of leiden tot dubbelingen en vooral veel papierwerk? Hoe verhoudt dit zich tot de nationale strategie, die ook nog moet worden opgesteld? Het CDA hecht eraan dat deze instrumenten elkaar versterken en niet onnodig bijdragen aan extra regeldruk. We hadden het er al over.

De minister heeft in de schriftelijke vragenronde aangegeven dat kleinere entiteiten in het kader van het tegengaan van regeldruk zelf kunnen afwegen of zij de risicobeoordeling laten samenvallen met andere wettelijke verplichtingen, bijvoorbeeld met de in de cybersecuritywet voorgestelde verplichtingen. Het CDA vindt het goed dat wordt gekozen voor maatwerk, maar hoe borgt de minister dat entiteiten weten wat ze wel en niet moeten doen en welke risicobeoordelingen echt noodzakelijk zijn en welke niet?

Voorzitter. Daarbovenop is er het beleid rondom de vitale infrastructuur, zoals de Aanpak vitaal van de NCTV, die sinds 2023 van kracht is. Mijn collega begon er al over. Ook deze aanpak richt zich op het vergroten van de weerbaarheid tegen allerlei soorten dreigingen. Kan de minister uiteenzetten hoe deze wet zich verhoudt tot de Aanpak vitaal en andere risicobeoordelingen die door deze wet tot stand moeten komen? Op welke manier worden overlap en versnippering voorkomen? Hoe wordt ervoor gezorgd dat er één samenhangend stelsel is, waarin duidelijk is wie waarvoor verantwoordelijk is? Ook ben ik benieuwd of de minister inmiddels met de Europese Commissie heeft gesproken over het borgen van informatie-uitwisseling, vertrouwelijkheid en betrouwbaarheid.

Voorzitter. Het lijkt het CDA een goede keuze om de vakministers verantwoordelijk te maken voor de toepassing van de elementen uit deze wet, terwijl de minister van Justitie en Veiligheid medeverantwoordelijk is. Dat betekent dat de risicobeoordeling door de vakminister wordt gedaan, wat aansluit bij de sectorspecifieke kennis die nodig is. Gaat de minister van Justitie en Veiligheid dan ook waarborgen dat de kennis- en informatiedeling tussen de vakministers en de kritieke entiteiten op orde is? Het lijkt mij nuttig dat zij niet steeds opnieuw het wiel moeten uitvinden en gebruik kunnen maken van eerder toegepaste best practices. Hoe gaat de minister voorkomen dat er te veel op eilandjes wordt gewerkt?

Voorzitter. Daarnaast wil ik kort stilstaan bij de uitvoerbaarheid van deze wet, met name voor kleinere en publiek-private kritieke entiteiten. Hoe wordt ervoor gezorgd dat verplichtingen proportioneel zijn en aansluiten bij de capaciteit en schaal van deze organisaties? Op welke wijze ondersteunt de overheid kritieke entiteiten bij het versterken van hun weerbaarheid, bijvoorbeeld via richtsnoeren of kennisdeling? Ook ben ik benieuwd wat voor Nederland de precieze gevolgen gaan zijn van de niet-tijdige implementatie van de CER-richtlijn. De oorspronkelijke deadline was 17 oktober 2024. Wordt Nederland daarvoor inderdaad een boete opgelegd? Zijn andere lidstaten ook nog steeds bezig met de implementatie of loopt alleen Nederland achter?

Tot slot over dit eerste wetsvoorstel. Een goede samenhang tussen fysieke en digitale weerbaarheid is essentieel. In een wereld waarin dreigingen steeds vaker hybride van aard zijn, kan een fysieke verstoring niet los worden gezien van cyberdreigingen. We zien deze wet dan ook als een belangrijke bouwsteen die goed moet aansluiten op andere wetgeving, zoals op de Cyberbeveiligingswet, waar ik het straks over ga hebben. Hoe gaat de minister deze samenhang borgen in de praktijk? De weerbaarheid van kritieke entiteiten is geen luxe, maar een noodzaak. Met deze wet zetten we een stap vooruit.

Vervolgens wil ik ingaan op de Cyberbeveiligingswet, waarmee Nederland de digitale kant van de NIS2-richtlijn implementeert. Het CDA vindt cybersecurity van grote waarde. We hebben de afgelopen week in het nieuws gezien wat de impact kan zijn. Van organisaties die essentiële diensten

leveren mag je verwachten dat ze hun digitale veiligheid op orde hebben. Dat geldt des te meer voor entiteiten die onze samenleving draaiende houden. Denk aan je telefoonprovider, je bank, de energieleverancier en de afvalinzamelaar, maar ook aan de gemeente. Het is goed dat er een zorgplicht komt en dat we meldplichten en toezicht aanscherpen. Het raakt aan de weerbaarheid van onze samenleving. Tegelijkertijd geldt dat we door dit wetsvoorstel wel weer extra verplichtingen opleggen. Dat kan noodzakelijk zijn, maar dan moeten we het stelsel wel robuust en uitvoerbaar maken. Juist wat dat betreft wil ik vandaag een paar punten uitlichten.

Allereerst noem ik samenhang, variatie en overlap in het toezicht. Het kabinet erkent dat overlap in het toezicht niet altijd te voorkomen is en dat, als er verschillende toezichthouders zijn, overlap zo veel mogelijk beperkt moet worden door afstemming, samenwerkingsafspraken én structureel overleg. Dat betekent in de praktijk: verschillende verplichtingen, verschillende toezichthouders en mogelijk ook verschillende interpretaties. Toezicht zal worden uitgeoefend door sectorale toezichthouders, die in meer of mindere mate al ervaring hebben op dit gebied van cyberbeveiliging. De mate en kwaliteit van het toezicht zullen, zeker in het begin, waarschijnlijk wisselend zijn. De Autoriteit Persoonsgegevens geeft aan dat als zij naast de NIS2-toezichthouders ook bevoegd is, niet duidelijk is wie er voorgaat bij het opleggen van een eventuele boete. Daarom vraag ik de minister hoe de coördinatie er in de uitvoering precies uitziet. Specifieker: is het voor organisaties helder wie wanneer hun eerste aanspreekpunt is bij toezicht, handhaving en incidentafhandeling met betrekking tot de Cyberbeveiligingswet?

De Afdeling advisering van de Raad van State vroeg in dit verband terecht om duidelijkheid over de invulling van de coördinerende rol en de taakafbakening in dit stelsel met vele sectoren en partijen. Het CDA wil dat dit niet alleen op papier, maar ook in de praktijk strak geregeld is, juist om stapeling te voorkomen. Ik vraag daarom om een toezegging: kan de minister ervoor zorgen dat de samenwerkingsafspraken tussen toezichthouders tijdig publiekelijk, of anderszins, duidelijk zijn, zodat organisaties vooraf weten waar zij aan toe zijn? Denk hierbij ook aan de kosten die, volgens het ATR, dat toeziet op het verminderen van de regeldruk, verbonden zijn aan kennisname van hoe het werkt en aan een eventuele beveiligingsscan of beveiligingsaudit.

Het volgende onderwerp is AI-gedreven cyberbedreigingen. Het CDA wil een punt aanstippen dat ook in ons gesprek met de Cyber Security Raad nadrukkelijk naar voren kwam. De razendsnelle ontwikkelingen rondom artificial intelligence vergroten niet alleen onze mogelijkheden aan de verdedigende kant, maar ook de slagkracht van aanvallers. Gecoördineerde cyberaanvallen met een groot aantal AI-agents liggen op de loer. Juist daarom is het van belang dat kennis over dreigingen, kwetsbaarheden en aanvalspatronen veel sneller en structureler worden gedeeld. Die kennisdeling is tot nu toe te beperkt en te versnipperd, zowel tussen

organisaties in Nederland als met landen die te maken hebben met vergelijkbare dreigingen. Is de minister bereid om te bezien hoe die kennisdeling steviger kan worden georganiseerd, niet alleen tussen uitvoeringsorganisaties en bedrijven hier, maar ook met landen als Frankrijk, Duitsland en het Verenigd Koninkrijk? In het kader van snel ontwikkelende, AI-gedreven cyberdreigingen is het van belang dat we niet allemaal afzonderlijk het wiel blijven uitvinden.

Dan kom ik bij de uitvoering door het Rijk. In de memorie van toelichting staat een tabel met de budgettaire gevolgen per departement. Die lopen structureel op tot bijna 83 miljoen euro. Dat is fors. Op zich is dat ook prima, als het leidt tot aantoonbaar betere ondersteuning, respons en toezicht. Betreft dit bijvoorbeeld ook de extra capaciteit bij onze uitvoeringsdiensten zoals de ILT en de NVWA, zodat hier ook geen vertragingen of wachtlijsten ontstaan? Ook vraag ik aan de minister welke concrete prestaties we hiervoor terug gaan zien in het toezicht. In dit verband is het ook relevant dat in de memorie wordt vermeld dat het Nationaal Cyber Security Centrum de uitvoerbaarheid haalbaar acht, mits aan de randvoorwaarden wordt voldaan. Een daarvan betreft een realistisch groeipad. Kan de minister toelichten hoe dat groeipad er nu uitziet? Hoe wordt geborgd dat toezicht en ondersteuning niet achterblijven bij de snelle verbreding van de doelgroep? Welke rol kan de Rijksinspectie Digitale Infrastructuur, de RDI, hierin pakken? Zij is naast toezichthouder namelijk ook uitvoerder, en kan helpen met die centrale regie.

Dan kom ik bij het risico op onbewuste non-compliance. De reikwijdte van dit wetsvoorstel is groot. In de stukken staat dat naar verwachting circa 8.100 organisaties grotendeels automatisch van rechtswege onder de Cyberbeveiligingswet zullen vallen. Ze worden niet individueel aangewezen en niet actief op de hoogte gesteld. Ze zullen zelf moeten beoordelen of ze onder de wet vallen, met ondersteuning van een zelfevaluatietool. Dit creëert een risico dat het CDA heel serieus neemt: een risico op onbewuste non-compliance. Dat gebeurt niet uit onwil, maar omdat organisaties simpelweg niet doorhebben dat ze onder de wet vallen, zeker als ze onderdeel zijn van een concernstructuur of als hun dienstverlening net op een grens zit. Ook kunnen organisaties twijfelen of ze het goed doen en dit willen laten toetsen, om eventuele overtredingen op een later moment te voorkomen. Is de minister bereid om met name het mkb en kleinere gemeenten hierin te faciliteren? Hoe voorkomen we dat juist de kwetsbare organisaties met minder capaciteit en expertise achterblijven?

Het is ook mooi als bedrijven elkaars geleerde lessen kennen. Ik refereerde daar net al even aan. Het werkt natuurlijk altijd goed als de ene ondernemer het de andere vertelt. Op die manier is een hack of een andere kwetsbaarheid geen taboe, maar sta je samen sterker en maak je ook je medewerkers digibewust en -bekwaam.

We hebben ook de oproep ontvangen om organisaties die objectief kenbaar tot taak hebben om de dreigingsinformatie en de informatie over

cyberincidenten te delen, de zekerheid te geven dat ze ook onder de wet aangemerkt zullen worden als een relevante partij. Kan het kabinet zekerheid geven over de status van zulke schakelorganisaties in Nederland? Hierin zit ook een element van wederkerigheid. We mogen veel vragen, maar dan moet de overheid ook leveren. Duidelijkheid, praktische hulpmiddelen en uniformiteit in de uitleg en het toezicht zijn hierbij onze uitgangspunten.

Dan de onderwijsinstellingen. De CDA-fractie heeft eerder gevraagd naar de bepalingen over onderwijsinstellingen. In de nota naar aanleiding van het verslag geeft de regering aan te hebben besloten dat de bekostigde hbo- en wo-instellingen onder de reikwijdte van de wet worden gebracht zonder onderscheid te maken tussen instellingen met kritieke onderzoeksactiviteiten. Dit gebeurt mede vanwege de samenwerking en onderlinge afhankelijkheid en vanwege de uitvoerbaarheid. Tegelijk wordt de aanwijzing van deze instellingen als een belangrijke of essentiële entiteit nog nader uitgewerkt. Mijn vraag is: bedoelt de regering dat de instellingen als geheel worden aangewezen of dat alle instellingen in deze categorie onder het regime moeten vallen, ongeacht profiel, risico en aanwezigheid van de kritieke onderzoeksactiviteiten? Hoe borgt de minister proportionaliteit, uitvoerbaarheid en de heldere criteria daarbij? Er leven hierover ook zorgen in de sector. Universiteiten van Nederland wijst op de administratieve lasten, het risico op dubbelingen en de onduidelijkheid, juist in een tijd van financiële druk. Ook SURF heeft aandacht gevraagd voor de werkbaarheid en het voorkomen van extra administratieve lasten. Het CDA zoekt hierin een duidelijke middenweg. Als we onderwijs aanwijzen, doe het dan op een manier waarop het voor iedereen werkt en wordt voortgebouwd op hun eerdere inspanningen.

Dan kom ik bij gekwalificeerde vertrouwensdiensten. De Autoriteit Persoonsgegevens heeft haar zorgen met ons gedeeld over de verwerking en het bewaren van persoonsgegevens. In de NIS2-richtlijn staat dat lidstaten essentiële en belangrijke entiteiten moeten aanmoedigen om gekwalificeerde vertrouwensdiensten te gebruiken. In gewone taal gaat het om digitale middelen die helpen om online zekerder vast te stellen met wie je zakendoet en of informatie of documenten echt en betrouwbaar zijn. Voor dit soort vertrouwensdiensten bestaan al heel veel Europese regels, maar ik zie nog niet duidelijk hoe Nederland het gebruik hiervan nu actief wil stimuleren. Kan de minister daarop reflecteren? Is hij bereid toe te zeggen de Kamer daarover te informeren en bijvoorbeeld voor de zomer met een brief te komen?

Tot slot, voorzitter. Ik rond af. Het CDA steunt beide wetsvoorstellen in hun doel: het versterken van de weerbaarheid van onze samenleving, zowel fysiek als digitaal. Maar grote wetten met een grote reikwijdte moeten ook begrijpelijk, uitvoerbaar en proportioneel zijn. Als we veel vragen van organisaties, moet de overheid ook zichtbaar leveren, zodat organisaties weten waar ze aan toe zijn. Ik hoor graag de reactie van de minister op de gestelde vragen en de gevraagde toezeggingen.

Dank u wel.

De **voorzitter**:

Dank u wel voor uw bijdrage. Dan gaan we naar mevrouw El Boujdaini van D66.

Mevrouw **El Boujdaini** (D66):

Dank u wel, voorzitter. Cyberveiligheid en weerbaarheid van kritieke entiteiten klinkt voor veel mensen als iets abstracts, als iets voor experts en techbedrijven, maar niets is minder waar. Cyberveiligheid gaat over het dagelijks leven van mensen, over of je 's ochtends je pinpas kan gebruiken, of je de trein naar je werk haalt en of het licht het nog doet wanneer je thuiskomt. Het gaat over vertrouwen, erop vertrouwen dat de systemen waar we elke dag op leunen, het gewoon doen. Stel je namelijk eens voor dat dat vertrouwen wegvalt. Stel je voor dat het betalingsverkeer platligt, drinkwatervoorzieningen, de energievoorzieningen of telecomnetwerken uitvallen en mensen letterlijk in het donker zitten zonder verwarming, bereik of toegang tot informatie. Dat zijn reële scenario's, die we in Europa al hebben zien gebeuren. Juist daarom is de weerbaarheid van onze kritieke entiteiten geen technisch detail, maar een maatschappelijke randvoorwaarde. Als we dit niet goed regelen, zijn het niet systemen die falen. Mensen dragen de gevolgen en hebben er last van.

Voorzitter. Voor D66 betekent dit dat we de digitale infrastructuur net zo serieus moeten beschermen als onze fysieke infrastructuur. Daarom spreken we vandaag ook over de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet. Dat is hard nodig, want Nederland loopt achter met de implementatie, terwijl de dreiging toeneemt. Deze wetten moeten ervoor zorgen dat kritieke entiteiten, zoals energievoorzieningen, drinkwatervoorzieningen, gemalen en telecombedrijven beter beschermd zijn bij en voorbereid zijn op incidenten, dat organisaties risico's in beeld hebben, maatregelen nemen en samenwerken om schade te beperken, en dat gemeentes en veiligheidsregio's weten wat hun te doen staat. De vraag is niet óf we onze weerbaarheid versterken, maar hóé we dat gaan doen, met wetgeving die ambitieus is, maar ook helder en uitvoerbaar. We kunnen digitaal en fysiek weerbaarder worden. Dat vraagt om een balans tussen veiligheid en uitvoerbaarheid, tussen toezicht en vertrouwen, tussen Europese verplichtingen en nationale aanpak. In dat licht wil ik vandaag een aantal punten bespreken. Allereerst sta ik stil bij de kwestie rondom Odido. Daarna bespreek ik de Wet weerbaarheid kritieke entiteiten, vervolgens de Cyberbeveiligingswet en tot slot hoe deze wetten volgens onze fractie nog robuuster kunnen worden.

Ik begin bij Odido, voorzitter. De Odidokwestie benadrukt waarom wij vandaag debatteren over deze wetten. Het maakt pijnlijk duidelijk hoe kwetsbaar onze digitale infrastructuur is als beveiliging tekortschiet. Wanneer gegevens van miljoenen mensen op straat belanden, raakt dat niet alleen hun privacy, maar ook het vertrouwen in de overheid en bedrijven, met risico's als identiteitsfraude, misbruik en langdurige onzekerheid. Dit raakt mensen dus echt. De Odidokwestie laat ook zien dat wetgeving op zichzelf niet genoeg is. Vanuit de Telecomwet zijn er al een meldplicht en een zorgplicht rond cyberveiligheid, maar uiteindelijk moet het dus in de praktijk goed gaan en moet het gaan leven. Daarom mijn vraag: hoe gaan we ervoor zorgen dat de consequenties zo klein mogelijk zijn bij dit soort datalekken van zo'n omvang? Immers, helemaal voorkomen kan jammer genoeg niet. Ziet de minister dan ook dat de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten de kans op dit soort datalekken kunnen verkleinen?

Voorzitter. Het grootschalige incident van Odido staat niet op zichzelf. Daar is veel misgegaan, maar een cyberaanval kan iedere sector overkomen. Naar verwachting zullen ruim 8.100 organisaties onder de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten vallen. Dat vraagt om een zorgvuldige wetsbehandeling, zodat onze cruciale sectoren beter voorbereid zijn op cyberbedreigingen en daar snel op kunnen reageren. Zo voorkomen we dat incidenten zoals bij Odido een nieuwe realiteit worden, of in ieder geval de consequenties ervan.

Voorzitter. Ik zei het al in mijn inleiding: de digitale wereld staat onder druk, met gevolgen voor onze fysieke veiligheid. De Wet weerbaarheid kritieke entiteiten beoogt deze veiligheid te waarborgen door organisaties die diensten aanbieden die cruciaal zijn voor het goed functioneren van onze maatschappij hier ook aan te laten voldoen. Een groot deel hiervan was ook al het geval onder de Aanpak vitaal. In plaats van vitale aanbieders worden er onder de nieuwe wet zogenaamde kritieke entiteiten aangewezen, of althans: zij moeten zichzelf aanwijzen. Dat zijn dus organisaties die een of meerdere essentiële diensten aanbieden die onze maatschappij draaiende houden. Wanneer dit wordt verstoord en uitvalt door een cyberaanval, heeft dat dus grote gevolgen voor mensen. Het is daarom van groot maatschappelijk belang dat de overgang van de Aanpak vitaal naar de Wet weerbaarheid kritieke entiteiten helder is voor organisaties. Daarom mijn volgende vragen. Welk deel van de Wet weerbaarheid kritieke entiteiten vervangt de Aanpak vitaal en hoe verhouden deze twee regimes zich straks ten opzichte van elkaar? Zijn straks alle vitale aanbieders kritieke entiteiten onder de Wwke? Welke organisaties worden daar eventueel nog aan toegevoegd? Tot slot. Is er een verschil tussen een kritieke entiteit en een essentiële entiteit onder de Cyberbeveiligingswet? Een kritieke entiteit is namelijk ook automatisch een essentiële entiteit onder de Cyberbeveiligingswet.

Verder wil ik toch nog aandacht vragen voor digitale soevereiniteit, want weerbare kritieke entiteiten zijn belangrijker dan ooit, met name in het licht van het maatschappelijk debat over digitale soevereiniteit. Er moeten strategische keuzes worden gemaakt: van wie wil je digitale diensten afnemen en waarvoor? Waar deze worden ingekocht, doet er daadwerkelijk toe. Digitale soevereiniteit gaat ook verder dan alleen de overheid. Dat laten deze wetten zien. Het gaat om de keuzes die andere organisaties en bedrijven maken, want alleen wanneer overheid, samenleving en bedrijven hier samen aan werken, worden we als Nederland digitaal weerbaar. Veel organisaties, dus ook de kritieke entiteiten, staan voor hetzelfde vraagstuk als de overheid. Neem de betaalinfrastructuur, ziekenhuizen en onderwijsinstellingen. Hoe moeten zij digitaal soeverein worden? Kunnen we misschien een gezamenlijke aanpak maken? Daarom mijn volgende vraag: kan de minister aangeven of er gewerkt gaat worden aan een aanpak om deze kritieke entiteiten ook meer digitaal soeverein te maken? Zo niet, is de minister bereid om dit te doen?

Voorzitter. Dan wil ik mijn licht nog laten schijnen op de particuliere beveiligingsbedrijven. Zij zijn ook vaak uitvoerders van weerbaarheidsmaatregelen bij kritieke entiteiten. Vanuit die hoek hebben we ook verschillende geluiden gehoord. Dit zijn bedrijven die werken aan toegangscontroles, bewaking en detectie, maar bijvoorbeeld ook aan personeelsbeveiliging en crisisbeheersing. Scherp hebben wat hun positie is in het kader van de Wwke is dus cruciaal. Kan de minister toelichten of en hoe de structurele betrokkenheid van de particuliere beveiligingssector bij oefeningen en scenario's voor incidenten wordt geborgd, zodat we met z'n allen goed voorbereid zijn? Kan de minister ook uiteenzetten of en hoe deze private beveiligingsbedrijven meer duidelijkheid kunnen krijgen over hun rollen, verantwoordelijkheden en aansprakelijkheden bij de implementatie van deze wetten? En kan de minister toelichten hoe wordt geborgd dat er heldere afspraken komen over de noodzakelijke informatie-uitwisseling tussen publieke crisisorganisaties, kritieke entiteiten en private veiligheidsbedrijven tijdens een crisis?

De heer **Van den Berg** (JA21):

Ik hoor mevrouw El Boujdaini van D66 net een punt maken over de behoefte van bedrijven aan soevereiniteit. Ze vroeg of de minister daar eventueel werk van wil maken. Hoe ziet mevrouw El Boujdaini dat voor zich in het kader van deze twee wetten? Ik vind het belangrijk, maar hoe ziet mevrouw El Boujdaini dat in het kader van deze twee wetten voor zich?

Mevrouw **El Boujdaini** (D66):

Ik denk dat deze twee wetten heel goed laten zien hoe belangrijk het is dat wij onze kritieke entiteiten beschermen. Volgens onze fractie gaat dat verder dan alleen kijken naar wat hun taken zijn; het gaat ook om waar zij daadwerkelijk gebruik van maken. We hebben de afgelopen maanden gezien dat het uitmaakt voor welke leveranciers en aanbieders je kiest. Dat geldt ook voor overheidsorganisaties. Ook wij als overheidsorganisatie kunnen als "kritieke entiteit" bestempeld worden. Daarom vind ik het belangrijk dat wij een stukje verder kijken: voor welke leveranciers kiezen zij, en brengt dat misschien ook bepaalde risico's met zich mee? Ook dat kan er namelijk voor zorgen dat er bijvoorbeeld bepaalde cyberdreigingen om de hoek liggen.

De **voorzitter**:

De heer Van den Berg, volgende interruptie.

De heer **Van den Berg** (JA21):

Zou dat ook in het kader van artikel 18 van het Cyberbeveiligingsbesluit zijn, dat de vergaande bevoegdheid geeft aan de overheid om bedrijven in het kader van de nationale veiligheid te dwingen om bepaalde diensten niet meer af te nemen of juist wel af te nemen? Moet ik dat dan zo zien?

Mevrouw **El Boujdaini** (D66):

Het woord "dwingen" heb ik niet gebruikt. Ik denk in eerste instantie dat het goed is om te kijken naar een aanpak hiervoor. Of dat dan meteen afdwingbaar is of niet, ligt er eigenlijk aan of de wet daarop wordt aangepast. Ik vraag op dit moment niet om een amendement hierop. Dat heb ik ook niet. Ik stel eerst de vraag aan de minister of hij bereid is om zo'n aanpak op te zetten. Daarna kunnen we verder kijken, denk ik, en bezien wat we daadwerkelijk kunnen verplichten.

De heer **Van den Berg** (JA21):

De vraag was meer of u daartoe bereid bent. Daar hoor ik geen duidelijk antwoord op, maar wel de vraag aan de minister om het wellicht te verplichten. Ik ben alsnog benieuwd naar de eigen visie van mevrouw El Boujdaini op hoe we in het kader van deze wet, die echt gaat over cyberbeveiliging en over weerbare kritieke entiteiten, die soevereiniteit zouden kunnen stimuleren. Ik zou niet willen zeggen "borgen", omdat dat losstaat van deze wet. Ik probeer gewoon uit te denken hoe we dat praktisch zouden kunnen inpassen.

Mevrouw **El Boujdaini** (D66):

Volgens mij zijn deze wetten er juist voor dat wij als samenleving zo veilig mogelijk ons leven kunnen leiden, dat onze gegevens veilig staan en dat organisaties met een maatschappelijke verantwoordelijkheid, bijvoorbeeld in de energievoorziening, het verkeersmanagement of telecombedrijven, vanuit hun eigen systemen veilig zijn vanbinnen, zodat zij ons die veiligheid ook kunnen garanderen. Nogmaals, ik denk dus dat we daar wel naar moeten kijken, omdat het daadwerkelijk uitmaakt welke software en systemen je inkoopt als organisatie en wat er vervolgens wordt gebruikt om ons als samenleving die veiligheid te kunnen garanderen.

Dit is natuurlijk een voorbeeld dat vaker wordt gebruikt, maar we hebben vorig jaar allemaal gezien hoe het Internationaal Strafhof is geraakt door Microsoft. Een aantal mensen daarvan kon ineens hun diensten niet meer gebruiken, omdat ze waren gesanctioneerd. Ik denk dat dat soort voorbeelden heel erg tekenend zijn. We moeten niet willen dat bepaalde kritieke entiteiten ook zo kwetsbaar kunnen zijn en zo afhankelijk zijn in hun dienstverlening aan ons, omdat zij een keuze hebben gemaakt voor een bepaalde leverancier. Het klopt dat daarover niks staat in deze wetten, vandaar dus ook mijn vraag aan de minister; ik zou in het kader van de veiligheid die we moeten kunnen garanderen, wel willen vragen om een aanpak.

De **voorzitter**:

Mevrouw El Boujdaini, u kunt verder met uw betoog.

Mevrouw **El Boujdaini** (D66):

Dan ga ik het over de Cyberbeveiligingswet hebben. Het is goed dat we deze wet gelijktijdig behandelen met de Wwke. Een kritieke entiteit onder de Wwke is ook een essentiële entiteit onder de Cyberbeveiligingswet. Dat gezegd hebbende wil ik het ook hebben over het lokaal bestuur, want het lokaal bestuur is onze fractie veel waard. Wij zetten gemeenten dan ook graag in hun kracht.

Stelt u zich eens voor dat de aansturing van gemalen wordt verstoord en dat dit wateroverlast veroorzaakt in woonwijken, of dat verkeersmanagementsystemen worden gehackt en het niet meer doen, wat chaos betekent in het verkeer. Het zijn dan dus gemeenten die moeten ingrijpen om de inwoners te beschermen en de orde in hun eigen gemeente te herstellen. De burgemeesters zijn daar met de veiligheidsregio's verantwoordelijk voor. Zij moeten wel weten wat er precies aan de hand is en wat de oorzaak van het incident is, ook om in de toekomst preventieve

maatregelen te kunnen nemen. Juist daarom is de uitvoering van de Cyberbeveiligingswet zo cruciaal.

Die wet is zo sterk als de informatie die wordt gedeeld en de partijen die daarop kunnen handelen. Daarom vinden wij het belangrijk dat de burgemeesters en de veiligheidsregio's weten wat zich afspeelt binnen de gemeenten, om zo veiligheid te kunnen waarborgen. De minister geeft in de schriftelijke beantwoording echter aan dat de Cyberbeveiligingswet het NCSC geen ruimte biedt om informatie te delen die geen betrekking heeft op de eigen cyberveiligheid van de gemeente. Dat betekent dat de gemeente als organisatie wel wordt geïnformeerd over de eigen cyberveiligheid, maar niet over wat zich op het gebied van cyberveiligheid afspeelt bij belangrijke en essentiële entiteiten binnen de gemeentegrenzen, tenzij er sprake is van nationale opschaling van een incident. Juist die informatie hebben gemeenten nodig om de lokale impact van cyberbedreigingen op de openbare orde en veiligheid binnen hun gemeentegrenzen te kunnen duiden.

Om die reden heb ik hierover een amendement ingediend. Wij begrijpen dat dit ook een extra verantwoordelijkheid is voor het NCSC, maar zij beschikken al over deze informatie en wij vragen of zij deze informatie willen delen met de burgemeesters en de voorzitters van de veiligheidsregio's. Hiermee wordt voorkomen dat gemeenten ieder afzonderlijk aanvullende afspraken moeten maken met bepaalde organisaties binnen hun gemeentegrenzen. Dit versterkt de aanpak van cyberincidenten die gevolgen hebben voor de openbare orde en veiligheid. Het zorgt er ook voor dat gemeenten zich veel beter kunnen voorbereiden op crisisincidenten binnen hun gemeentegrenzen in de toekomst. Wij kijken dan ook uit naar de appreciatie van de minister.

Voorzitter. De Wwke en de Cyberbeveiligingswet zien op het Europees deel van Nederland; mijn collega Van den Berg begon er ook al over. Dat is wetstechnisch begrijpelijk, omdat het hier gaat om de implementatie van Europese regelgeving. Tegelijkertijd mogen we het belang van het Caribisch deel van Nederland niet uit het oog verliezen. Ook in het Caribisch deel is het van groot belang dat de digitale weerbaarheid wordt versterkt. Zo was er in 2022 nog een ransomwareaanval op het enige water- en elektriciteitsbedrijf van Sint-Maarten. Door de aanval verloor het bedrijf de toegang tot financiële data, terwijl er geen recente back-up beschikbaar was. Tot op de dag van vandaag ervaren mensen op Sint-Maarten hiervan nog de consequenties. Op Aruba was er ook een ransomwareaanval, op een ziekenhuis. De aanval verstoorde de bedrijfsvoering en de operationele uitvoering van werkzaamheden. Dit had impact op de dienstverlening en de patiënten.

Gemeenschappelijke voorzieningen, overheidsdiensten en bedrijven in het Caribisch deel van Nederland zijn ook in toenemende mate afhankelijk van digitale systemen. Het is daarom van belang dat ook inwoners van het Caribisch deel kunnen rekenen op een passend niveau van digitale bescherming en weerbaarheid. Er is al een veiligheidsstrategie voor het Koninkrijk der Nederlanden. Dat is een goed begin, maar biedt nog niet

genoeg handelingsperspectief. Ik heb daarom de volgende vragen aan de minister. Werkt het kabinet aan een concreet plan of een routekaart om te komen tot een cybersecuritystelsel voor het Caribisch deel van Nederland dat zo veel mogelijk aansluit op het niveau van digitale bescherming en weerbaarheid hier in Nederland? Wordt het Caribisch deel van het Koninkrijk dan betrokken bij de ontwikkeling van dat stelsel? Zo ja, op welke manier? Kan de minister aangeven welk tijdpad het kabinet voor ogen heeft om tot een dergelijk beschermingsniveau voor het Caribisch deel te komen?

Voorzitter. Ik ben bijna klaar, maar wil het graag nog even hebben over toezicht. Wij hechten aan een ambitieus maar ook helder en uitvoerbaar pakket maatregelen om onze cyberveiligheid te versterken. Voor onze fractie geldt daarbij vereenvoudigen waar kan, maar maatwerk waar nodig. Afstemming tussen toezichthouders is essentieel om dubbele toezichtlasten te voorkomen. De minister geeft aan dat hierover sectorale samenwerkingsafspraken zullen worden gemaakt en dat de instanties die toezicht houden op de Cyberbeveiligingswet samenwerken in het door de RDI opgerichte directeurenoverleg, het DTDW, om zo te werken aan een gezamenlijke en meer geharmoniseerde aanpak van toezicht op digitale weerbaarheid. Mijn fractie ziet dit als wenselijke stappen. Tegelijkertijd hebben we nog wel enkele vragen. Worden deze samenwerkingsafspraken uiteindelijk in alle sectoren gemaakt of zijn er sectoren waar dat nog niet gebeurt? Zijn in die zin daarmee dan alle blinde vlekken in het toezicht in kaart gebracht en straks ook opgelost? Hoe verhouden de coördinerende taak en de stelselverantwoordelijkheid van de minister zich tot het directeurenoverleg? Tot slot: in hoeverre worden organisaties die onder dit toezicht vallen, betrokken of geconsulteerd bij de afspraken die in dit overleg worde gemaakt?

Voorzitter, ik rond af. Deze wetten gaan uiteindelijk over mensen, over de zekerheid dat je 's ochtends gewoon naar je werk kunt, dat het licht het doet, dat je water uit de kraan krijgt en dat je erop kunt vertrouwen dat je gegevens veilig zijn. De Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet zijn belangrijke stappen om die zekerheid beter te beschermen in een wereld waarin dreigingen steeds minder zichtbaar zijn maar steeds ingrijpender worden. Duidelijke regels waar organisaties mee uit de voeten kunnen, zijn daarom belangrijk, opdat verplichtingen niet alleen op papier werken maar ook in de praktijk. Als we dat goed doen, bouwen we aan weerbaarheid en voorzieningen die blijven draaien. Mijn fractie ziet daarnaar uit.

Dank u wel.

De **voorzitter**:

Dank voor uw bijdrage. U heeft verder geen interrupties. Dan gaan we naar de heer Van Dijk van de PVV.

De heer **Emiel van Dijk** (PVV):

Dank u wel, voorzitter. De Cyberbeveiligingswet, de Nederlandse vertaling van de Europese NIS2-richtlijn, is Brusselse regelgeving in optima forma. Het is weer een berg aan nieuwe regels die vanuit de EU worden opgelegd aan Nederland. Het is waar, op papier klinkt het niet eens zo heel slecht: zorgen dat onze digitale systemen beter beschermd zijn tegen hackers, ransomware en andere cyberdreigingen. Want ja, niemand wil dat de stroom uitvalt, treinen stilvallen, ziekenhuizen platliggen of banken gehackt worden. Maar zoals altijd met EU-regelgeving wordt het een enorme administratieve rompslomp, met hoge kosten voor vooral bedrijven maar uiteindelijk ook voor de gewone Nederlander.

Voorzitter. Deze wet treft zo'n 8.100 bedrijven en organisaties in Nederland. Dat zijn er veel meer dan onder de oude regels. Denk aan energiebedrijven, vervoerders, luchtvaart, spoor, wegen, scheepvaart, drinkwaterbedrijven, afvalbedrijven, ziekenhuizen, zorginstellingen, banken en financiële partijen, waarbij er deels overlap is met andere regels, grote cloudaanbieders, internetproviders, socialmediaplatforms, zoekmachines, postbedrijven; noem het maar op. Maar denk ook aan gemeenten, waterschappen en sommige onderwijsinstellingen. Er wordt onderscheid gemaakt tussen essentiële entiteiten en belangrijke entiteiten. Veel middelgrote en grote bedrijven vallen er automatisch onder als ze meer dan 50 werknemers hebben of meer dan 10 miljoen euro omzet draaien.

Wat moeten die bedrijven dan straks allemaal doen? Ze krijgen een zorgplicht, moeten risico's inschatten, maatregelen nemen om hacks te voorkomen, systemen beter beveiligen, personeel trainen, hun toeleveranciers beschermen en zorgen voor een veilige ontwikkeling van software en fysieke beveiliging van servers. Bij een serieuze cyberaanval of storing moeten ze binnen 24 uur melding doen bij de overheid via een centraal loket, gevolgd door updates en een eindrapport. Bestuurders moeten een cybertraining volgen en zich blijven bijscholen. Er komt ook een registerplicht en er komen periodieke checks door toezichthouders. Wie niet meewerkt, riskeert boetes tot 10 miljoen euro of 2% van de wereldwijde omzet. Dat zijn forse bedragen, die een bedrijf kapot kunnen maken.

De kosten zijn niet mals. Bedrijven betalen het grotendeels zelf: audits, externe adviseurs, nieuwe software of hardware. Uit schattingen blijkt dat middelgrote bedrijven structureel zo'n 1.246 uur per jaar kwijt zijn aan al die regels. Dat is meer dan een halfjaar fulltime werk voor één persoon. Eenmalig investeren ze gemiddeld rond de €25.000 en grote bedrijven zelfs €44.000 of meer, plus jaarlijks tienduizenden euro's aan doorlopende kosten. Voor kleine ondernemers in de keten sijpelt het allemaal door. Hogere prijzen voor energie, zorg, vervoer of onlinediensten: uiteindelijk betaalt de burger het, met hogere rekeningen, duurdere boodschappen en tragere leveringen. En dat terwijl Nederland al kampt met hoge lasten en een economie die kraakt

onder de regeldruk. De PVV is daar geen voorstander van. Wij zeggen hier nee tegen. Cyberbeveiliging is belangrijk -- we willen immers geen Chinese of Russische hackers die ons land lamleggen -- maar dit moet nationaal en slim gebeuren, en niet via dictaten uit Brussel met een one-size-fits-allaanpak ...

De **voorzitter**:

Meneer Van Dijk, u heeft eerst een interruptie van mevrouw Zwinkels, als ik het goed heb, en dan van mevrouw Martens-America.

De heer **Emiel van Dijk** (PVV):

... die kleine en grote bedrijven de nek omdraaien.

De **voorzitter**:

Ik had dus niet een goed moment gevonden! Ik dacht van wel. Mevrouw Zwinkels, van het CDA.

Mevrouw **Zwinkels** (CDA):

Op zich is het een terecht punt dat we de regeldruk in de gaten moeten houden. Daar heb ik ook een punt van gemaakt in mijn inbreng. Alleen kan ik helemaal niet volgen welke kant dit nu op gaat met de PVV. We hebben vorige week ook nog een debat gehad over Odido, naar aanleiding van de hacks die daar hebben plaatsgevonden. Dan blaast de PVV ook hoog van de toren met "hoe kan dit?", "schande", en weet ik het allemaal. Dan denk ik bij mezelf: deze wetgeving is er juist voor bedoeld om dat grotendeels te voorkomen en ervoor te zorgen dat die bedrijven zoals Odido ook een zorgplicht hebben naar hun klanten, burgers die daar hun data hebben. Het kan niet allebei waar zijn. Waarom is de PVV dan niet bereid om hierin te investeren? Zien zij niet in dat hiermee heel veel risico's voor die bedrijven, en daarmee ook voor onze burgers, voorkomen kunnen worden?

De heer **Emiel van Dijk** (PVV):

Die databeschermingsregelgeving bestond bij Odido natuurlijk al. Zij hebben zich niet aan de regels gehouden. Ze hebben data onnodig lang opgeslagen. Dat is dus met de huidige regelgeving al niet voorkomen. De huidige regelgeving verbiedt het om bepaalde data, zoals kopieën van paspoorten, rijbewijzen en adresgegevens, langer dan nodig te bewaren. Als dat nu al niet gehandhaafd wordt, wat heeft het dan voor nut om er nog zo'n hele lading

Brusselse regelgeving op los te laten, terwijl Odido in die zaak juist bewezen heeft dat het al niet werkt zoals het nu gaat?

Mevrouw **Zwinkels** (CDA):

Heel simpel: dat is ook helemaal de reden waarom we dit beleid moeten aanscherpen met elkaar, waarom deze maatregelen nodig zijn. We zien in de praktijk dat het niet toereikend is. Dan hoor ik de PVV ook zeggen "wat een schande dat er allemaal boetes worden uitgedeeld", maar dan denk ik bij mezelf: ja, maar het is voor een bedrijf ook vrij duur als ze allemaal losgeld moeten betalen en als ze voor het dilemma komen te staan of ze dat wel of niet gaan doen. Ik vraag me dan af of Odido volgens de PVV geen boete zou moeten betalen. Ik volg gewoon totaal niet waar het pleidooi van de PVV naartoe gaat. Ik hoop toch echt dat er wel iets meer steun kan komen voor hoe we samen weerbaarder gaan worden.

De heer **Emiel van Dijk** (PVV):

We zijn er als partij nog niet over uit wat we met dit pakket doen. We hinken op twee benen. Aan de ene kant is het belangrijk dat je actie onderneemt voor je eigen cyberveiligheid. Aan de andere kant is dit weer Brusselse overregulering. Ik denk dat we de Europese Unie niet nodig hebben om zelf onze zaakjes op orde te hebben. Om terug te komen op het Odido-verhaal: dat is natuurlijk een compleet andere situatie. Er was en is regelgeving actief. Ondanks dat we die regelgeving op haar plek hebben, heeft het bedrijf zich daar niet aan gehouden. De logica om dan in een reflex te schieten van "de regelgeving die we nu hebben en die nu in werking is, daar houdt men zich niet aan, dus komen we met een hele lading aan extra regelgeving", snap ik echt niet. Ik ga daar dan ook niet in mee.

Mevrouw **Zwinkels** (CDA):

Mijn punt ten aanzien van die boetes blijft staan. Daarvan denk ik: we regelen nu juist met elkaar om daar op een structurele manier een aanpak voor te hebben.

Tot slot over Europa. Juist voor bedrijven die in meerdere landen actief zijn, is het echt heel erg belangrijk dat we niet allerlei verschillende interpretaties hebben, maar dat we zulke Europese wetgeving juist implementeren op een zo uniform mogelijke manier en dat harmoniseren, zodat bedrijven daarvan op aan kunnen en weten waar ze aan toe zijn. Ik denk dat het juist heel erg belangrijk is dat alle lidstaten niet los van elkaar allemaal regels gaan bedenken, maar dat we dit op een vergelijkbare manier uitvoeren. Ik denk dat dat juist kan leiden tot minder regeldruk.

De heer **Emiel van Dijk** (PVV):

Het zou kunnen leiden tot minder regeldruk, maar in de praktijk zien we altijd dat de Europese Unie niet zorgt voor minder regeldruk, maar enkel voor meer regeldruk. Om terug te komen op het verhaal van Odido: als je 7 miljoen adressen en persoonsgegevens en dergelijke op straat hebt laten komen door nalatigheid, doordat je je niet aan de huidige fungerende regelgeving hebt gehouden, dan zal je daar een boete voor kunnen krijgen. Dat vind ik heel normaal. De klanten van Odido hebben namelijk gewoon het nakijken gehad. Als wij ergens een keuze moeten maken, kiezen we niet voor het bedrijf dat nalatig is geweest, maar voor de burger die de komende jaren misschien geconfronteerd wordt met identiteitsfraude en allerlei andere problemen rondom bankzaken en hypotheken en noem het maar op.

Mevrouw **Martens-America** (VVD):

Ik luister met een enigszins verontrustend gevoel naar de bijdrage van de PVV, ook omdat ik denk dat we anno 2026 de fase wel voorbij zijn dat je bedrijf veilig houden niet meer is dan een extra schuifje op de voordeur. Je verdienmodellen vinden op een andere manier plaats dan fysiek. Dat vraagt ook dat we misschien tien of twintig stappen vooruit moeten zetten, in plaats van afwachten. Maar goed, iedere fractie kiest hier natuurlijk haar eigen woorden. Het goede nieuws is -- dat is ook niet altijd zo -- dat ik de PVV zich zorgen hoor maken over onze ondernemers en het bedrijfsleven. Mijn glas is dus halfvol. Ik grijp dat graag met beide handen aan. Is de heer Van Dijk het niet met mij eens dat we juist deze ondernemers gaan helpen door op Europees niveau te zorgen dat de wet- en regelgeving gelijkgetrokken wordt? Daardoor wordt het concurrerende speelveld tussen Europese landen namelijk steeds minder en daar worden de Nederlandse ondernemers alleen maar beter van. Ik snap de zorgen over afspraken op Europees niveau dus niet zo goed. Misschien kan de heer Van Dijk die nog even toelichten.

De heer **Emiel van Dijk** (PVV):

Een gelijk speelveld is natuurlijk perfect. Dat is waar de Europese Economische Gemeenschap juist voor opgericht is. Het is nu echter een politieke unie geworden. Ze willen een grote geopolitieke speler zijn en zullen niks nalaten als het gaat om regelgeving uitstrooien over de lidstaten om daar verder stapjes in te zetten. Gelijk speelveld: ja. Politieke unie: nee.

Uw eerste vraag ging over de ondernemers. U zei dat we aan de kant van de ondernemers staan en dat dat positief was. Ja, dat heeft u goed geconstateerd.

Mevrouw **Martens-America** (VVD):

Uw antwoord is natuurlijk in volledige abstractie. Dat snap ik, want u, zeg ik via de voorzitter, geeft geen antwoord op mijn vraag. U maakt er een geopolitiek vraagstuk van. Dat mag. Mijn vraag is: welke negatieve gevolgen zouden Europese ondernemers op dat niveau en op dit moment ondervinden van afspraken op een gelijk speelveld? Welk nadeel gaan onze bedrijven hiervan ondervinden?

De heer **Emiel van Dijk** (PVV):

Dat is een beetje het probleem. Dat gelijke speelveld hadden we onder de EEG kunnen bereiken. Dat hoeft niet via de Europese Unie te lopen. Ik snap niet wat daar zo complex aan is. Europese economische samenwerking is prima, maar op het moment dat dat zich ontwikkelt tot een Brusselse hegemonie op alle facetten van het leven, vind ik dat we daar paal en perk aan moeten stellen. Daarom twijfelen wij ook of dit wetsvoorstel, dat een uitvoering is van de NIS2-richtlijn wel de manier is om dat aan te pakken.

Mevrouw **Martens-America** (VVD):

Ik ga proberen mijn vraag nog simpeler te stellen. Ik denk dat het wel belangrijk is dat, ondanks wat je vindt van de rol van de Europese Unie ... Mijn fractie maakt zich ook zorgen over nationale koppen op Europese wet- en regelgeving. Dit is nou juist zo'n wet die ervoor gaat zorgen dat wij elkaar op Europees niveau niet blijven beconcurreren, omdat we elkaar aan dezelfde wet- en regelgeving moeten houden, die -- laten we heel eerlijk zijn -- van essentieel belang zijn voor u en ik, zeg ik via de voorzitter, om ervoor te zorgen dat onze persoonsgegevens daadwerkelijk veilig blijven. Welk nadeel gaan ondernemers ondervinden van Europese wet- en regelgeving als het gaat om uw en mijn veiligheid?

De heer **Emiel van Dijk** (PVV):

Dat heb ik net aangestipt. Dat gaat over investeringen die ze moeten doen, over 1.250 uur per jaar die ze kwijt zijn aan regelgeving, over de meldplicht, over alle administratieve rompslomp en over de trainingen en de bijscholingen en dergelijke die ze moeten gaan doen. Nogmaals, dat heeft dus niet voorkomen dat de data van Odido, dat zich gewoon aan nationale regelgeving had moeten houden, alsnog op straat hebben gelegen. Ik zie dus het nut van extra regelgeving niet, als we de huidige regelgeving niet handhaven. Een gelijk speelveld is prima, maar dan wel in beperkte mate.

De heer **Van den Berg** (JA21):

Ik wil de heer Van Dijk toch wel bijvallen, want ik hoor volgens mij iets wat ik net ook inbracht in mijn bijdrage, namelijk dat er inderdaad een gelijk Europees speelveld moet zijn en dat dit niet moet leiden tot extra lastendruk. Mijn vraag aan de heer Van Dijk van de PVV is dan ook hoe hij er nou naar kijkt dat je in andere landen een meer coöperatieve houding ziet bij de toezichthouders en er dus niet gelijk wordt beboet, en dat het hier in Nederland nog niet zo strak in de wetgeving is opgenomen, waardoor dit wel zo kan uitpakken?

De heer **Emiel van Dijk** (PVV):

Daar ben ik geen voorstander van. Ik zou zeggen dat er iets van coulance moet zijn. Het voorbeeld van Frankrijk dat u noemde, vind ik op zich de meest logische manier, zeker als je continu met ontwikkelingen te maken hebt die van invloed zijn op hoe die wet uitwerkt voor bedrijven. Het lijkt me dat je niet meteen boetes gaat opleggen. We zijn er in Nederland heel goed in om meteen overal boetes, aanmaningen, brieven en dergelijke voor te sturen. Ik zou daarin wat milder zijn richting bedrijven in de uitwerking van deze wet, waarbij de vraag is of die doorgaat en in welke mate die doorgaat.

De heer **Van den Berg** (JA21):

Dan nog een open vraag aan de heer Van Dijk: wat zou er nou, ten opzichte van hoe die nu voorligt, concreet aan deze wet moeten veranderen om die wel acceptabel te laten worden voor de heer Van Dijk en de PVV?

De heer **Emiel van Dijk** (PVV):

Ik had liever gezien dat het initiatief vanuit Nederland zelf was gekomen zonder dat wij daarvoor dictaten vanuit Brussel over ons heen gestrooid krijgen. Dan kunnen we namelijk echt maatwerk leveren en hebben we niet te maken met het grotere ideaal van een Europees gelijk speelveld. Wat heeft een universiteit in Griekenland er voor baat bij dat een universiteit in Nederland dezelfde cyberbeveiligingsstandaarden heeft? Ik zie daar het nut absoluut niet van in, maar tegelijkertijd moeten we ons er wel aan conformeren en geeft het ons een enorme bureaucratische rompslomp, die uiteindelijk aan de burger wordt doorberekend.

Mevrouw **El Boujdaini** (D66):

Er ligt heel veel nadruk op dat het iets heel negatiefs is voor bedrijven, maar als we dit vanuit Europa aanpakken, creëren we dus juist dat gelijke speelveld. Ik hoor de heer Van Dijk ook veel over de boetes, maar tegelijkertijd heeft de Europese Commissie ook ingeschat dat het per jaar 180

miljard euro tot 290 miljard euro zou besparen op cyberincidenten. Dat is wat al die cyberincidenten ons op dit moment kosten. Ik denk dat het dus ook heel veel kansen biedt. Als we dit goed doen, goed oppakken en ervoor zorgen dat het uitvoerbaar is, kunnen we bedrijven hierin juist helpen, doordat het hen niet meer zulke grote bedragen kost aan wat ze zelf moeten regelen op het moment dat er dus zo'n cyberincident heeft plaatsgevonden. Ik denk dat deze wetgeving ons enorm gaat helpen in het kader van "voorkomen is beter dan genezen". Is de heer Van Dijk dat met mij eens? Ziet hij wat ik net uitlegde ook zo?

De heer **Emiel van Dijk** (PVV):

Ik begrijp waar mevrouw El Boujdaini van D66 vandaan komt, maar ik denk dat in essentie het grootste verschil tussen D66 en de PVV is dat wij liever zien dat we de regie nationaal houden, dat we onze soevereiniteit behouden en dat als we vinden dat we geld zouden kunnen besparen door onze cyberveiligheid op orde te krijgen, het initiatief uit Nederland zou moeten komen, vanuit het ministerie of vanuit de Tweede Kamer als het ministerie het zou nalaten. Nationale koppen op Brusselse regelgeving doen natuurlijk iets anders dan een gelijk speelveld creëren. Als ik de lijn van de collega's volg, zouden we met de implementatie van de NIS2-richtlijn nu een gelijk speelveld moeten krijgen. Maar wat gebeurt er dan? Dan worden er nationale koppen op gezet. Ik snap dat niet, want die nationale koppen zorgen juist voor een ongelijk speelveld. Je hebt dus een gigantische toename van bureaucratie en regelgeving voor bedrijven, en tegelijkertijd creëer je een ongelijk speelveld door die nationale koppen erop te zetten.

Mevrouw **El Boujdaini** (D66):

Ik denk dat wat de heer Van Dijk benoemt, het verschil tussen de PVV en D66, wel klopt. Wij zien inderdaad zeker wel de meerwaarde van deze wetgeving vanuit Europa. Het mooie is juist dat we nog steeds de ruimte krijgen voor maatwerk voor ons eigen Nederland, om te kijken wat er het beste past bij onze bedrijven en organisaties hier in Nederland en wat ten goede komt aan onze samenleving. Als laatste zou ik dus aan de heer Van Dijk willen vragen om misschien toch ook te kijken naar de voordelen van deze wetgeving voor bedrijven. Het is namelijk echt niet alleen negativiteit en het biedt ook echt wel kansen, ook om geld te besparen.

De heer **Emiel van Dijk** (PVV):

Afsluitend. Wij zijn altijd bereid om te kijken naar de voordelen. Wij zien hier echter alleen meer nadelen. Toch nog even een reactie. U zegt: "Het is mooi dat we van de EU de ruimte krijgen om ons eigen beleid te voeren." Dat is

dus precies het grote verschil tussen de partij van mevrouw El Boujdaini en de PVV. Wij vinden het principe van soevereiniteit zo belangrijk dat het eigenlijk schandalig is dat we hier van de EU een kruimeltje krijgen om ons eigen beleid te mogen voeren. Dat zou niet zo moeten zijn. Wij zouden in ons eigen land moeten kunnen bepalen hoe we de dingen aanvliegen, en niet blij moeten zijn dat de EU ons de ruimte heeft gegeven om binnen de richtlijnen en verordeningen die zij over ons uitstrooit nog kleine keuzes te maken.

De **voorzitter**:

Meneer Van Dijk, u kunt verder met uw betoog.

De heer **Emiel van Dijk** (PVV):

Dank u wel, voorzitter. Leg de focus op de echte vitale systemen van de overheid, de gemeenten, kritieke infrastructuur, Defensie en telecom. Bescherm die sectoren streng met Nederlandse oplossingen die passen bij onze situatie en dus niet met EU-lagen die innovatie remmen en kosten opdrijven. Wij staan voor Nederland eerst. Sterke cyberweerbaarheid: ja, maar betaalbaar en zonder dat hardwerkende ondernemers en burgers opdraaien voor Brusselse overregulering. Stop met de eindeloze regelstroom die onze economie verder verzwakt. Investeer in eigen capaciteit bij de politie, inlichtingendiensten en experts om dreigingen aan te pakken in plaats van bedrijven te dwingen tot dure administratieve oefeningen. Wij willen een Nederland waarin bedrijven kunnen ondernemen zonder overmatige bureaucratie vanuit de EU en waarin de burger niet direct op kosten wordt gejaagd door elke nieuwe EU-richtlijn. Cyberdreigingen aanpakken: absoluut, maar doe het op zijn Nederlands -- proportioneel en zonder de gewone man en het mkb kapot te reguleren.

Dank u wel.

De **voorzitter**:

Dank voor uw bijdrage. Dan vraag ik even aan de heer Van den Berg of hij het voorzitterschap over wil nemen om het woord te kunnen geven aan het lid Kathmann van GroenLinks-Partij van de Arbeid.

Voorzitter: Van den Berg

De **voorzitter**:

At your service. Ik geef het woord aan mevrouw Kathmann van GroenLinks-Partij van de Arbeid.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dank u wel, voorzitter. Veiligheid, weerbaarheid, het toverwoord "cyber": het is het heetste onderwerp in de politiek -- eindelijk, zou ik willen zeggen. Een onzekere wereld dwingt tot actie, en maar goed ook, want het denken over onze infrastructuur moet radicaal anders. De computers waar onze economie en ons land op draaien, zijn eindelijk onderwerp van gesprek. Het doet ertoe wie de baas is over die computers en hoe ze beveiligd worden, want door die kabels, chips en serverkasten blijft ons land overeind. Of je nou een ziekenhuis, een postbedrijf of een middelgrote gemeente bent, je hebt een verantwoordelijkheid. Te lang is dat niet zo geweest. Grote bedrijven en de overheid kochten hun ICT-spullen in alsof het kantoorartikelen waren, niks meer dan pennen, printpapier en een nietmachine. Achteraf zijn we daar waarschijnlijk naïef in geweest, want in onze digitale infrastructuur kunnen we het hardst geraakt worden. Eén gerichte cyberaanval en een deel van onze economie functioneert niet meer. Eén leverancier die zich terugtrekt en gemeenten liggen op hun gat. Digitale spionage en ddos-aanvallen zitten inmiddels in de gereedschapskist van iedere boef. Maar ook ons denken over fysieke veiligheid moet beter, want sabotage ligt niet alleen digitaal op de loer. Een onbeschermde datakabel, een deur die te gemakkelijk opengaat of een hek waar je zo een gat in knipt: ook dat zijn kwetsbare plekken. Op die manier kunnen boeven toegang krijgen tot een sluis, een laboratorium met kostbare spullen of een gemeentehuis. Als je rommelt met zulke belangrijke organisaties, heeft dat hele grote gevolgen. Dat zijn namelijk kritieke entiteiten, die onmisbaar zijn voor ons land.

Kortom, ik wil maar zeggen: goed dat deze wetten er zijn. GroenLinks-Partij van de Arbeid steunt de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. Met deze wetten gaan we samen met andere Europese landen één plan trekken voor onze cyberveiligheid en voor de fysieke veiligheid van belangrijke organisaties. Veiligheid hoort thuis aan elke bestuurstafel. Dat geldt met name voor cyberveiligheid. Deze wetten dwingen dat af.

Maar met hoe groot deze wetten zijn, begin ik even bij stap één. Ik vraag de minister het volgende. Kan hij heel concreet samenvatten wat er straks eigenlijk gaat veranderen als deze wetten worden aangenomen? Wat is nou precies een essentiële entiteit, een belangrijke entiteit en een kritieke entiteit? Kan hij per entiteit een paar voorbeelden opnoemen? Op welke manier wordt Nederland weerbaarder en veiliger van deze wetten? Wat gaan burgers hiervan merken? Wat gaan de entiteiten merken van de nieuwe wetten? Wat is de zorgplicht? Wat is de meldplicht? Hoe wordt er toezicht gehouden? Welke crisisteams, de zogenaamde CSIRT's, worden er straks

aangewezen voor de sectoren? Welke nieuwe moeten er nog worden opgericht?

Ik stel die vragen omdat ik wil dat mensen begrijpen wat er nu eigenlijk gaat veranderen. Wij moeten duidelijk maken hoe we burgers veilig houden. Cyberveiligheid en weerbaarheid is iets voor ons allemaal. Het zijn niet zomaar buzzwords voor bestuurders en politici om over te kletsen. Het is een belofte die wij aan burgers geven: dat wij hun recht op een veilig leven ook serieus nemen.

Ik wil wat langer doorgaan over de positie van de burger. Deze wetten richten zich namelijk volledig op wat er binnen organisaties moet gebeuren. Het betreft de maatregelen die je moet nemen om je beter te beschermen. Dat is de zogenaamde zorgplicht. Ook gaan ze over hoe je melding moet maken als er iets misgaat. Dat is de meldplicht. Maar we leven niet op een eiland met alleen maar bestuurders, CEO's en toezichthouders, die samen afspraken maken. Een datalek of een aanval op infrastructuur is allang geen kwestie van bedrijfsvoering meer. Het is een kwestie van nationaal belang. Het heeft gevolgen voor mensen.

Neem het voorbeeld van een groot datalek. We hoeven daar niet ver voor te zoeken, want we hebben het meegemaakt met de miljoenen Odidoklanten van wie de gegevens nu op straat liggen en met alle vrouwen die getroffen zijn door het datalek bij het bevolkingsonderzoek baarmoederhalskanker. Terwijl de ministeries, de toezichthouders en de organisaties druk met elkaar in de weer zijn, blijven de slachtoffers eigenlijk nog steeds bekaaid achter. Ze hebben hele terechte, praktische vragen. Wat moet ik doen om mezelf te beschermen? Waar moet ik op letten? Welke telefoontjes of mailtjes kan ik niet meer vertrouwen? Kan ik mijn burgerservicenummer vervangen om fraude te voorkomen? Die vragen krijg ik als Kamerlid binnen van de mensen die ik vertegenwoordig. Vergeet niet: hoe belangrijk de cyberveiligheid van bedrijven en overheden wel niet is, als het misgaat zijn individuele klanten en burgers de allergrootste pineut.

Met name denk ik aan de kwetsbare groepen in Nederland, mensen voor wie hun privacy een essentiële veiligheidsgarantie is. Denk aan slachtoffers van huiselijk geweld van wie het huisadres is gelekt, aan publieke personen die anonimiteit nodig hebben om ongestoord door de dag te komen of aan lhbti'ers die voor hun eigen veiligheid zijn wegverhuisd en nu met één zoektocht op het darkweb weer vindbaar zijn geworden. Ik wil een wet die hun rechten beschermt.

Daarom pleit ik ervoor om een wettelijke nazorgplicht te introduceren. In zo'n wet staat precies hoe slachtoffers na een grote cyberaanval of een datalek geïnformeerd en geholpen moeten worden. Als we niet steviger opkomen voor slachtoffers, dan verliezen zij hun vertrouwen in de overheid en in de grote bedrijven die onmisbaar zijn in ons land. Zonder dat vertrouwen breekt precies datgene af wat we met deze nieuwe wet willen beschermen.

Daarom vraag ik het volgende van de minister. Hoe kijkt hij naar het maken van een nieuwe wet met een nazorgplicht? Is hij het met me eens dat dit de rechten van slachtoffers van een datalek meer zekerheid kan geven? Is de positie van slachtoffers goed genoeg vastgelegd in de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten? Welke verplichtingen gelden er voor de overheid en entiteiten als een cyberaanval een hoop slachtoffers maakt? Op welke hulp kunnen slachtoffers zich beroepen? Is de minister bereid om te verkennen hoe hun rechten wettelijk vastgelegd kunnen worden met een nazorgplicht voor de overheid en entiteiten?

Dan het basispakket digitale veiligheid. Eerder pleitte ik ook voor een basispakket digitale veiligheid: een bundel van cybersecuritysoftware die is gemaakt door het Nederlandse bedrijfsleven en die centraal wordt aangeboden door de overheid in samenwerking met diezelfde bedrijven. Ik weet dat er op de markt genoeg oplossingen zijn, maar als cybersecurity alleen is weggelegd voor mensen die weten wat een VPN is en die snappen welke wachtwoordmanager het beste uit de test komt, dan constateer ik dat het gewoon niet toegankelijk genoeg is. De opdracht is helder: ook mijn oude buurvrouw moet online veilig zijn, niet alleen de techneut die thuis zijn eigen mailserver draait. GroenLinks-Partij van de Arbeid wil een toegankelijk pakket met een VPN, een wachtwoordmanager, antivirussoftware en een adblocker, gemaakt met gebruiksgemak voor elke doelgroep en makkelijk te installeren op meerdere apparaten. De motie die ik hierover heb ingediend, heb ik aangehouden, omdat de staatssecretaris Digitale Economie tijd nodig had om die te appreciëren. De appreciatie is er nog niet, dus ik probeer het nog een keer in dit debat. Is de minister het met me eens dat cyberveiligheid ook voor individuele burgers bereikbaar, betaalbaar en begrijpelijk moet zijn? Hoe kijkt de minister naar mijn voorstel voor een basispakket digitale veiligheid? Op welke manier zou dit samen met de markt vormgegeven kunnen worden? Is de minister bereid om samen met Economische Zaken en Binnenlandse Zaken te bezien hoe een basispakket digitale veiligheid gerealiseerd kan worden?

Dan kom ik weer bij de wetten. Die roepen bij mij een hele hoop vragen op. Hoe blij ik ook ben dat ze er zijn, ook al zijn ze een beetje laat: er valt nog wel wat op af te dingen, onder andere wat betreft de hele waslijst aan dingen die nog moeten worden uitgewerkt. Denk hierbij aan de hoeveelheid belangrijke zaken die niet eens in de wet staan, maar in regeltjes die nog moeten worden gemaakt. Ook een hoop praktische dingen en randgevallen zijn nog niet duidelijk. Ik zal er hier niet een aantal noemen, want dat gaan heel lang duren. Maar ik heb hier al één, twee, een heleboel pagina's voor me met onduidelijkheden. Ik noem bijvoorbeeld een meldportaal dat nog niet duidelijk is, de rol van de toezichthouder en de nieuwe, maar nog onbekende taken van het Nationaal Cyber Security Centrum. Dit is echt nog maar een hele kleine greep uit alles wat nog boven de markt hangt. Over wetten die zo lang in de oven hebben gezeten, had ik eerlijk gezegd meer zekerheid verwacht.

We tuigen een heel nieuw systeem van regels, toezicht en handhaving op, maar niemand weet nog hoe dat er precies uit gaat zien.

We nemen dus straks misschien wetgeving aan zonder te weten of het allemaal uitvoerbaar is. In gesprekken met bedrijven, gemeenten en andere organisaties die straks aan de wetgeving moeten voldoen, hoor ik dit ook terug als een van hun grootste zorgen. Herkent de minister die kritiek op de uitwerking van de wetten? Hoe zorgt hij ervoor dat de naleving niet een groot fiasco wordt als de wetten eenmaal zijn aangenomen? Kan de minister aangeven wanneer hij verwacht dat alle punten zijn uitgewerkt? Ik heb die punten net dus niet allemaal opgenoemd, maar die zijn wel genoemd in allerlei memories van toelichting en beantwoordingen. Is de minister bereid om schriftelijk een overzicht te geven van alle punten waarop de wetten nog nader worden uitgewerkt, samen met een tijdlijn van wanneer we een uitwerking kunnen verwachten?

Dit brengt me meteen bij een belangrijk punt van kritiek op de wetten. Er is namelijk ontiegelijk veel uitgewerkt in lagere regelgeving. In normale mensentaal zegt dat eigenlijk: we hebben een wet geschreven, maar hoe je die regels eigenlijk naleeft, moet je maar zien in de bijlagen die we later nog wel gaan opsturen. In sommige gevallen snap ik dat echt, maar als het gaat om twee wetten die zo lang op zich hebben laten wachten en waar zo veel urgentie achter zit, snap ik het minder goed. We bespreken twee wetten met zware verplichtingen, die heel veel open eindjes hebben. Toen ik in de schriftelijke ronde vroeg waarom de zorgplicht pas in het Cyberbeveiligingsbesluit -- dat is dus die bijlage waar ik het over had -- staat, kreeg ik als antwoord dat dat alleen maar om een uitwerking gaat. Dat is niet helemaal zo. Ten eerste is de uitvoering ervan knetterpolitiek. Het is één ding om op te schrijven dat je meer aan je veiligheid moet doen, maar het is nog steeds een politieke vraag wát je dan precies moet doen. Wanneer ben je als entiteit cyberveilig? Hoe bescherm je je fysieke infrastructuur? Kortom, wanneer voldoe je aan de wet? Die vragen moet je duidelijk kunnen beantwoorden. Als je de hele kern van een wet pas in lagere regels uitwerkt, is dat moeilijk.

Gelukkig hebben we het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten goed ontvangen. Maar ook daar staan nog zaken in die niet uitgewerkt zijn. Voor de entiteiten én voor de volksvertegenwoordiging is dat lastig controleren. Ik heb daarover een aantal vragen. Heeft de mate waarin dingen nog verder worden uitgewerkt te maken met haast? Is het te laat implementeren van de richtlijnen een reden geweest om veel dingen in lagere regelgeving te bepalen? Heeft de minister overwogen om meer zaken al op het niveau van de wet duidelijk te maken? Waarom is de afweging gemaakt om vooral de zorgplicht, een heel zwaar middel, in algemene maatregelen van bestuur te zetten? Is de minister bereid om in de evaluatie van de wetten, die ergens in de komende vier of vijf jaar plaatsvindt, te bezien of er met een wetswijziging alsnog meer zaken in de wet zelf geregeld kunnen worden, en wat daar de voor- en nadelen van zijn? Dit is waarom ik

voor allebei de wetten een amendement heb ingediend om een voorhangprocedure toe te voegen. Als er iets aan de uitwerking van de wetten verandert, specifiek als het gaat om de zorgplicht, dan moet de Kamer daarover geïnformeerd worden. Zo wordt de uitvoering van de wetten beter controleerbaar en geven we onszelf de kans om in te grijpen als de wetten niet goed worden uitgewerkt. Hoe kijkt de minister naar mijn voorstel over het toevoegen van een voorhang voor de zorgplicht bij beide wetten? Hoe gaat hij ervoor zorgen dat de uitwerking van de twee wetten zorgvuldig, transparant en met zo veel mogelijk inspraak van zowel de entiteiten als de Kamer plaatsvindt?

In die lage regelgeving staat iets heel zwaars. Dat gaat om de interventiebevoegdheid.

De **voorzitter**:

Mevrouw Kathmann, ik zat al even te zoeken naar een moment, omdat ik uw vlammende betoog niet wilde onderbreken. Maar u heeft een interruptie van de heer Van den Berg van JA21 en dat ben ikzelf.

Ik hoor u steun uitspreken voor beide wetten, zowel voor de Cyberbeveiligingswet als voor de Wet weerbaarheid kritieke entiteiten. Maar ik hoor tegelijkertijd ook een bak aan kritiek, die ik terecht vind. Er zijn heel veel vragen. U zegt onder andere dat er een wettelijke nazorgplicht moet komen. U vraagt waarom het in lagere regelgeving is uitgewerkt en of er haast bij is geweest. Als u al die kritiekpunten heeft en er nog zo veel moet veranderen, waarom zou je dan aan de voorkant toch alvast steun uitspreken? Is dat niet de omgekeerde richting?

Mevrouw **Kathmann** (GroenLinks-PvdA):

Nee, de cyberveiligheid van Nederland, waar deze wetten een hoop voor gaan doen, is echt ongelofelijk belangrijk. Daar moet urgentie voor zijn en dat moeten we gewoon zo snel mogelijk met elkaar willen doen. Ik ben heel blij dat deze wetten er nu liggen. Ik heb alleen wel met volgens mij vier amendementen gepoogd om die onduidelijkheden eruit te halen via die voorhang. Dan worden we als Kamer heel goed geïnformeerd over de verdere uitwerking. Daar kunnen we dan nog dingen aan veranderen. U heeft ook gezegd: laten we de wet eerder evalueren. Ik heb de minister net gevraagd: kunnen we bij de evaluatie kijken of we dan nog dingen in de wet willen regelen in plaats van in lage regelgeving of bij algemene maatregel van bestuur? Er zijn nog een aantal dingen waarover ik per amendement of motie duidelijkheid probeer te scheppen. Het gaat mij vooral om die onduidelijkheid. Ik heb het idee dat de minister dat ook wel ziet. Dat blijkt uit de beantwoording van eerdere vragen. Ik hoop vooral dat we vandaag heel

veel zaken kunnen doen en dat we ook nog zaken kunnen doen als de wet geëvalueerd wordt.

De **voorzitter**:

Mevrouw Kathmann heeft dus wel het gevoel dat de wetten, als al die zaken worden doorgevoerd, allebei goed genoeg zijn om echt een bijdrage te kunnen leveren aan de cyberveiligheid van Nederland?

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ja, dat heb ik zeker. Dat is zeker zo als wij als Tweede Kamer onze controlerende taak beter kunnen borgen. Dat vind ik echt heel belangrijk. Ik ga het zo even hebben over de interventiebevoegdheid. Daar wil ik gewoon meer duidelijkheid over en ook, zoals ik net al zei, over de voorhang. Dat zijn op zich elementaire dingen, waardoor wij ons werk beter kunnen doen en we de wet misschien in een later stadium nog kunnen aanscherpen. En dan zou ik zeggen: zo snel mogelijk gaan met die banaan, want we kunnen gewoon niet langer wachten.

De **voorzitter**:

Dan geef ik als voorzitter het woord terug aan mevrouw Kathmann voor het vervolg van haar betoog.

Mevrouw **Kathmann** (GroenLinks-PvdA):

In die lagere regelgeving staat iets heel zwaars. Het gaat om de interventiebevoegdheid, oftewel om artikel 18 van het Cyberbeveiligingsbesluit en artikel 13 van het Besluit weerbaarheid kritieke entiteiten. Dit is een uitwerking van de zorgplicht die de vakminister de mogelijkheid geeft om diensten en producten te verbieden, oftewel de interventiebevoegdheid. Laat ik vooropstellen dat het helemaal geen gek idee is. Als we weten dat ergens een component in een systeem zit, dat er ergens een stukje software wordt gebruikt of dat er een bepaald onderdeeltje in de harde infrastructuur is dat ons kwetsbaar maakt, dan moeten we dat kunnen uitfaseren. GroenLinks-Partij van de Arbeid staat dus achter de interventiebevoegdheid, maar laten we wel wezen: het is een heel zwaar middel, dat niet even in een lagere regel moet worden neergezet, bijna uit het niks, als een onderdeeltje van de zorgplicht. Dat is eigenlijk een grote verrassing. Daarom heb ik twee amendementen ingediend: eentje voor de Cyberbeveiligingswet en eentje voor de Wet weerbaarheid kritieke entiteiten. Die amendementen doen niks anders dan de interventiebevoegdheid uit de lagere regels halen en netjes in de wet zetten.

Voor de Cyberbeveiligingswet stel ik voor om artikel 21a toe te voegen. Dat is letterlijk dezelfde tekst als de minister al wil plus een beetje. Ik stel namelijk twee extra dingen voor. Ten eerste stel ik voor dat ingrijpen door de vakminister een laatste redmiddel is, echt een last resort. Eerst moet vaststaan dat er geen andere maatregelen zijn die de risico's voor de nationale veiligheid wegnemen. Dat spreekt misschien voor zich, zou je denken, maar door dit in de wet te zetten voorkom je dat we dit zware middel zonder goede reden inzetten. Dat moet altijd gegrond zijn en dat zorgt voor rechtszekerheid voor entiteiten.

Ten tweede stel ik een inspanningsverplichting voor. De vakminister en het sectorale crisisteam, het CSIRT, moeten samen met de entiteit die iets moet afsluiten, kijken of er ondersteuning bij nodig is. Je kunt niet zomaar verwachten dat entiteiten dit in hun eentje kunnen doen, vooral als het gaat om een bijna onmisbaar deel van hun dienstverlening. "Er hoeft niks te gebeuren" kan ook een uitkomst zijn van de inspanningsverplichting. Als je een entiteit vraagt om iets helemaal uit te faseren, dan vind ik het de verantwoordelijkheid van de vakminister en het crisisteam om daarbij te helpen. Daarbij blijft de dienstverlening van de entiteit ook overeind.

Ik ga echt uit van de beste intenties bij het inzetten van de interventiebevoegdheid, maar de vakminister zomaar op zijn of haar blauwe ogen geloven, is volgens mij niet hoe wij hier met elkaar wetgeving moeten beoordelen. De manier waarop de bevoegdheid nu is opgeschreven, is dan ook echt te kort door de bocht. Met mijn amendement hoop ik op meer zekerheid. Politieke willekeur van het kabinet hoop ik ook te voorkomen, maar de mogelijkheid om in te grijpen blijft wel gewoon overeind, alleen met een paar nieuwe vangrails, zodat de vakministers niet uit de bocht kunnen vliegen.

Voor de Wet weerbaarheid kritieke entiteiten gaat het trouwens om een heel nieuw artikel 15a, dat een uitwerking is van de zorgplicht in artikel 15. Het amendement is vrijwel identiek, alleen gaat het om kritieke entiteiten en fysieke diensten en producten. In de inspanningsverplichting van dit amendement is er geen rol weggelegd voor de toezichthouder, omdat voor deze wet een groepje aangewezen ambtenaren de toezichthoudende partij is. Dat zou dus dubbelop zijn. Daarom is het de vakminister die dit samen met de entiteit uitzoekt.

Over mijn amendementen heb ik een paar vragen. Ten eerste ben ik heel benieuwd hoe de minister de amendementen beoordeelt. Het is vrijwel dezelfde tekst als in de lage regelgeving, maar dan in de wet. Is hij het met me eens dat we op deze manier een duidelijker kader geven aan de interventiebevoegdheid? Hoe kijkt hij specifiek naar de nieuwe toevoegingen, die stellen dat het een last-resortmaatregel moet zijn en dat er een inspanningsverplichting moet komen? Hoe kijkt de minister naar de mogelijkheid om, als dat nodig wordt geacht, ook financiële steun te leveren

bij het weren van een dienst of product? Is de minister daartoe bereid en, zo ja, wat is de hoogte van zo'n bijdrage zonder dat die staatssteun wordt?

Ik zeg het even hardop: deze amendementen zijn een uitgestoken hand, want mijn doel is duidelijk. De interventiebevoegdheid moet blijven, maar hoort thuis in de wet, met een duidelijke grens. Dit weegt voor mijn fractie zwaar. Ik hoop dan ook dat de minister niet met een harde "nee" komt, maar met mij meedenkt over hoe wij dit een beetje netjes in de wet kunnen krijgen. Zou hij anders in een schriftelijke beantwoording alternatieven kunnen noemen, mochten de amendementen niet op zijn steun kunnen rekenen?

Over de interventiebevoegdheid heb ik nog één grote vraag. GroenLinks-Partij van de Arbeid heeft duidelijk gemaakt dat een van onze grootste veiligheidsproblemen de totale eenzijdige afhankelijkheid van vooral Amerikaanse software en hardware is. De interventiebevoegdheid wordt ingezet als er sprake is van diensten of producten van een bedrijf uit een land dat op gespannen voet staat met Nederland, dat verplicht is om inlichtingen met de overheid te delen en uitgebreide toegang geeft tot onze systemen. Daar is nu dus eigenlijk volop sprake van. In ons land zijn wij massaal afhankelijk van Amerikaanse ICT-diensten, waardoor bedrijfsgeheimen en burgergegevens direct onder de reikwijdte van spionagewetten vallen. Denk aan de CLOUD Act, de Foreign Intelligence Surveillance Act en aan Executive Order 12333.

Over die interventiebevoegdheid heb ik wat vragen. Is de minister bereid om die bevoegdheid in te zetten om gevaarlijke afhankelijkheden in onze dienstverlening terug te dringen? Kan hij klip-en-klaar uitleggen waarom ICT-diensten uit de Verenigde Staten níet zouden voldoen aan de voorwaarden om deze interventiebevoegdheid in te zetten? Wanneer zou hier wel sprake van zijn? Kortom: kan de minister heel duidelijk zeggen wanneer hij bereid is om de interventiebevoegdheid in te zetten? Volgens mij is mijn punt duidelijk: hoe, wanneer en waarom de interventiebevoegdheid wordt ingezet, moet transparant en controleerbaar zijn. Ik roep de minister op om dit zo concreet mogelijk te maken voordat de wetten in werking treden.

Straks worden duizenden organisaties aangemerkt als entiteiten als zij onder de nieuwe wetten vallen. Bij de Cyberbeveiligingswet wordt uitgegaan van zo'n 8.100 essentiële en belangrijke entiteiten. Let wel op: in het Cyberbeveiligingsbesluit is sprake van 7.550 entiteiten. Ik hoor graag wat het echte aantal is. De Wet weerbaarheid kritieke entiteiten gaat uit van 500 organisaties die worden bestempeld als kritieke entiteiten. Er is dus wel een schatting gemaakt, maar een organisatie moet zelf uitzoeken of zij ook echt zo'n entiteit is. Organisaties moeten een vitaalbeoordeling uitvoeren om te achterhalen of zij daaronder vallen. Voor wetten die strenge, nieuwe verplichtingen opleggen, is dat toch best vrijblijvend. Mijn zorg is dat er straks organisaties zijn die helemaal niet weten of zij onder deze wet vallen. Daarover heb ik wat vragen. Hoe zullen alle entiteiten zich volgens de minister met zo'n vitaalbeoordeling identificeren? Ziet hij het risico dat er

organisaties zijn die de beoordeling niet doen en er dus niet van op de hoogte zijn dat zij onder de nieuwe wet vallen? Is er geen risico op onderrapportage doordat organisaties de beoordeling niet invullen om de verplichting uit de weg te gaan? Hoe snel verwacht de minister dat alle entiteiten in kaart zijn gebracht? Hoe gaat hij alle vermoedelijke entiteiten zover krijgen om die beoordeling in te vullen?

GroenLinks-Partij van de Arbeid vraagt zich af waarom het kabinet wél in staat is om zo'n schatting te maken, maar niet in staat is om die bedrijven proactief aan te schrijven met het simpele bericht "u bent vermoedelijk een entiteit; doe nu de test". Is de minister bereid om alsnog alle organisaties aan te schrijven waarvan hij volgens zijn eigen inschatting vermoedt dat zij entiteiten zijn? Kan hij via de voorzitter met de Kamer delen hoe hij de inschatting van het aantal entiteiten heeft gemaakt? Kan hij dit getal uiteenzetten per sector en laten zien hoe hij die organisaties gaat benaderen?

Er is al een hele waslijst aan handreikingen, handboeken, infosheets, brochures en onlinetools gemaakt over de NIS2-richtlijn en de CER-richtlijn. Kan de minister zeggen hoe vaak deze al zijn gebruikt? Is dat in lijn met wat hij verwacht? Worden de beschikbare hulpmiddelen nog gebundeld en op één centrale plek aangeboden, zodat organisaties heel makkelijk alle informatie kunnen vinden?

Het omschakelen van papier naar praktijk wordt een uitdaging. Met deze wet willen we alles opknippen in keurige sectoren met dezelfde standaarden voor de maatregelen die je neemt en de manier waarop je informatie deelt. Maar hoe graag we dat ook willen, we weten maar al te goed hoe weerbarstig de realiteit is. Volgens mij is al door een x-aantal partijen gevraagd hoe gemeentes dat dan zouden moeten doen. Dit stukje kort ik daarom in.

Wat overblijft, is de Uitvoerbaarheidstoets Decentrale Overheden. Die is niet uitgevoerd. Is de minister bereid om die wel uit te voeren voordat de wetten in werking treden? Wat gaat de minister doen om de rollen van vakministers, toezichthouders en de sector zo goed mogelijk vast te leggen? Wanneer en hoe worden deze stelselafspraken gemaakt?

De volgende vragen in mijn tekst kan ik volgens mij ook overslaan. Dat is al allemaal gevraagd.

Een praktisch punt waar entiteiten mee te maken krijgen, is het doen van een melding. Melding doen van een cyberaanval is straks niet meer vrijwillig; als je als entiteit aan een bepaalde drempelwaarde voldoet, is het verplicht. Ik kijk ernaar met het motto "je bent een held als je meldt", want we moeten echt zo veel mogelijk meldingen binnenkrijgen. Laten we ervan uitgaan dat iedereen melding doet als er iets ergs gebeurt. Dat moet zo makkelijk mogelijk zijn, het liefst op één gestandaardiseerde manier voor alle soorten meldingen, ook voor meldingen die je moet doen op grond van andere sectorale wetgeving of die volgen uit de AVG wanneer er sprake is van

persoonsgegevens. Kortom, ik pleit voor één integraal en overzichtelijk meldloket voor entiteiten.

Daarover heb ik een aantal vragen. Hoe kijkt de minister aan tegen één centraal meldloket voor alle soorten meldingen die entiteiten moeten doen? Zijn er mogelijkheden om dit goed te bundelen en, zo ja, wat voor soort meldingen kunnen centraal in één zo'n loket worden gebundeld? Is de minister bereid om tot één meldloket te komen voor zo veel mogelijk soorten meldingen, om het voor entiteiten zo makkelijk mogelijk te maken om informatie aan de toezichthouder door te geven? De meldingsbereidheid moet hoe dan ook omhoog. GroenLinks-Partij van de Arbeid vraagt zich af hoe het nu staat met de meldingsbereidheid. Kan de minister aangeven hoe het er nu voor staat met de meldingsbereidheid onder organisaties die een lek, aanval of kwetsbaarheid aantreffen? Wordt er in de meeste gevallen melding gemaakt?

Dan gegevensdeling. Daar zijn volgens mij ook al een aantal vragen over gesteld. Ik kijk even of ik mijn tekst hierover nog een beetje kan inkorten. De cyberveiligheid van de CSIRT's moet net zo waterdicht zijn als van alle entiteiten waar ze op toezien. Ik hoor de heer Van den Berg buiten de microfoon al "ja" zeggen. Heeft hij daar vragen over gesteld?

Wat betreft de bewaartermijn sluit ik mij aan bij de vragen van JA21. Ik heb nog wel de vraag hoe de minister erop toeziet dat de gegevens die de CSIRT's gaan verwerken, goed beveiligd worden. Kan hij vertellen welke technische veiligheidsmaatregelen hij neemt om daarvoor te zorgen? Over de bewaartermijn zijn al de nodige vragen gesteld.

De **voorzitter**:

Ik heb wel een vraag aan mevrouw Kathmann van GroenLinks-Partij van de Arbeid. U sprak over een centraal meldpunt en de veiligheidseisen bij de CSIRT's. U zei dat de veiligheid waterdicht moet zijn. Juist als zij die bijzondere gegevens heel erg lang bewaren, zijn zij zelf ook een doelwit, omdat vijandige mogendheden die gegevens bijvoorbeeld zouden willen hebben. Daar heb ik een amendement voor voorbereid. Daarin staat dat we minimale waarborgen moeten toevoegen voor onafhankelijk toezicht, zodat, als het onder een ministerie valt, datzelfde ministerie of een toezichthouder van dat ministerie er geen toezicht op kan houden. Dat is een beetje de slager die zijn eigen vlees keurt. Hoe kijkt mevrouw Kathmann naar die aanpak? Zou dat goed zijn?

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ja, dat zou een goede aanpak zijn. Ik ga zo met heel veel enthousiasme naar uw amendement kijken. Ik heb op dat terrein wat vragen overgeslagen om

tijd te winnen, maar die lopen we nu gewoon weer in. Ik ga dus zeker met veel enthousiasme naar uw amendement kijken.

De **voorzitter**:

Hartstikke mooi. Gaat u verder met uw betoog.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ook onmisbaar in ons informatielandschap zijn de gegevens die publiek-privaat worden gedeeld. Hoewel we trots kunnen zijn op alle bedrijven die hun kostbare gegevens nu al met autoriteiten delen, past het niet dat we voor ons dreigingsbeeld volledig afhankelijk zijn van private inlichtingen. Onze publieke instellingen moeten die competentie gaan kweken, maar die zijn daar niet van de ene op de andere dag toe in staat. Momenteel zijn er organisaties die volgens de wet data mogen uitwisselen met het Nationaal Cyber Security Centrum, de zogenaamde OKTT-organisaties. Nu is er wat onduidelijkheid ontstaan over of dit onder de nieuwe wetten nog steeds relevante partijen zijn die data mogen uitwisselen. Kan de minister bevestigen dat de OKTT-organisaties onder de twee nieuwe wetten nog steeds relevante dreigingsinformatie mogen ontvangen om te delen met hun achterban binnen de sectoren? Als dat niet het geval is, waarom dan niet, en hoe wordt die taak dan wel ingevuld?

De volgende grote zorg van GroenLinks-Partij van de Arbeid betreft de centen. Het verbeteren van je ICT-kennis, het opleiden van je bestuur, het opstellen van een cyberplan en het nemen van allerlei maatregelen om jezelf digitaal en fysiek te beschermen, komt met een prijskaartje. Er zijn straks duizenden organisaties die daarmee aan de bak moeten. Dat is kostbaar. Er komt ook een flinke nieuwe taak bij voor het bestaande personeel. Als organisaties zulke expertise van buiten moeten inkopen, vissen ze ook nog eens met z'n allen uit dezelfde vijver. Ik wil eigenlijk dat iedereen klaar is voor deze start zodra de wetten zijn aangenomen, met genoeg geld op de plank en een goed idee over welke stappen je als organisatie moet nemen om de wet te volgen.

Kan de minister helder schetsen wat er van entiteiten wordt verwacht in het eerste jaar nadat de wetten zijn aangenomen? Welke deadlines gelden er? Hoe moeten entiteiten of organisaties die dat waarschijnlijk zijn, zich voorbereiden op de nieuwe wetten? Hoe maken zij een realistische inschatting van de nieuwe taken en financiële lasten? Welke indicaties heeft de minister dat entiteiten voorbereid zijn op de nieuwe taken en financiële lasten van de nieuwe wetten? Verschilt deze paraatheid per sector? Waar zitten de risico's? Als er voor entiteiten praktische of financiële drempels zijn om aan de wet te voldoen, welke publieke taak heeft de minister dan om hen bij te staan?

Al die nieuwe taken komen met een nieuw stelsel van toezicht. Sommige bestaande inspecties en waakhonden worden uitgebreid. Voor sommige sectoren komen er geheel nieuwe toezichthouders. Dat is maar goed ook, want elke sector verdient een aanspreekpunt en een handhaver van de nieuwe wetten. GroenLinks-Partij van de Arbeid maakt vaker het punt dat cyberwetgeving te weinig oog heeft voor de positie van de toezichthouder. Veel te vaak wordt er gesteld dat er amper extra taken bij komen, dat het budget wel voldoende is en dat er altijd verdere afspraken gemaakt kunnen worden. Bij deze wetten ben ik er ook niet gerust op. Het toezicht staat in Nederland namelijk al onder druk en er gaan al heel veel incidenten aan ons voorbij omdat we de tegenmacht niet genoeg knaken geven voor al hun taken. Dat mag bij de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten niet gebeuren.

Kijk naar de Inspectie Gezondheidszorg en Jeugd, waarvoor nu al wordt gesteld dat er mogelijk meer geld nodig is om de naleving van de wet te kunnen controleren. Hoe kun je dat nou zeggen en vervolgens ook aangeven dat je het pas zeker zal weten nadat de wet in werking is getreden? Wat gaat de minister doen om toezichthouders, zoals de IGJ, van tevoren al zekerheid te geven over hun budget? Als blijkt dat toezichthouders onvoldoende geld hebben, hoe gaat de minister hen dan ondersteunen, zodat ze niet interen op hun eigen reserves?

Kijk bijvoorbeeld ook naar de ANVS, de nucleaire toezichthouder. Die stelt dat ze nu geen boetebevoegdheid heeft, maar wel onderdeel is van de wet. Ik kijk even naar mevrouw Faber. Had u daar nou vragen over gesteld? Dan kan ik die namelijk ook overslaan. Ja. Dan sluit ik me aan bij de vragen van mevrouw Faber. Dat scheelt weer heel veel tijd.

Hetzelfde geldt eigenlijk voor de Nederlandse Voedsel- en Warenautoriteit. Die heeft mevrouw Zwinkels, van het CDA, al genoemd. GroenLinks-Partij van de Arbeid sluit zich dus van harte aan bij die vragen.

Dan sluit ik me ook van harte aan bij de vragen over Caribisch Nederland, die door JA21 en D66 zijn gesteld. Het is namelijk echt van heel groot belang dat zij daar in ieder geval een stip op de horizon krijgen. Er waren hier vorig jaar een aantal vertegenwoordigers. Die zeiden ook: er zijn gewoon piraten actief en ze hebben niet meer zo'n lapje voor hun ogen, maar het zijn allemaal cyberpiraten; het wordt tijd dat wij ons hier ook in het Caribisch deel van het Koninkrijk maximaal tegen kunnen beschermen.

Het mag duidelijk zijn: GroenLinks-PvdA staat in voor de cyberveiligheid en de weerbaarheid van Nederland. Er woedt een oorlog achter de schermen. Van een van onze grootste economische spelers, onze onmisbare leveringsketens en onze volledige overheid mag je dan gewoon de opperste paraatheid verwachten, maar ik maakte al eerder het punt dat paraatheid niet alleen iets is voor bestuurders en CEO's, maar voor ons allemaal. Naast deze belangrijke wetgeving verwacht ik van het kabinet een plan voor de veiligheid van alle Nederlanders, met praktische, individuele oplossingen die

je veilig houden in de onlinewereld. Er is handelingsperspectief voor wat je zelf kan doen. Laten we ook toewerken naar een nazorgplicht, een wettelijke plicht voor het omgaan met een massaal datalek of een cyberaanval waarbij persoonsgegevens van Nederlanders massaal worden buitgemaakt. Cyberveiligheid houdt niet op bij het beheersen van risico's. Je moet nog veel meer doen. Je hebt als burger recht op informatie en hulp als je data worden gestolen van een bedrijf of overheid.

Ik kijk uit naar de beantwoording van de minister.

De **voorzitter**:

Ik zie verder geen interrupties meer. Dan wil ik mevrouw Kathmann hartelijk danken voor haar vurige bijdrage en geef ik het voorzitterschap graag aan haar terug.

Voorzitter: Kathmann

De **voorzitter**:

Dank. Ik kijk even naar rechts en naar de klok. Hoelang zou u willen schorsen, minister? Wij zullen dat zeker met een lunchpauze combineren. Ik denk dat een uur goed is. Ik kijk even naar links. Ja. Dan schorsen wij tot 13.30 uur.

De vergadering wordt van 12.25 uur tot 13.34 uur geschorst.

De **voorzitter**:

We gaan weer van start met het bespreken van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. We zijn bij de beantwoording door de minister, dus het woord is aan de minister.

Minister **Van Weel**:

Dank, voorzitter. U ziet hier een hele stapel papier voor mij liggen. U heeft in een paar uur meer dan 230 vragen afgevuurd over deze twee wetten. Dat is bijna twee keer zoveel als het aantal schriftelijke vragen dat over de wet is gesteld door uw Kamer. Daarmee wil ik aangeven dat als ik dit nu voorlees en ik één minuut per vraag neem, we al zo'n vierenhalf uur bezig zijn en dan heeft u nog geen interrupties kunnen plegen. Met uw welnemen zou mijn voorstel zijn dat ik door de vragen heen ga en dat ik probeer de vragen waarin feitelijk wordt gevraagd naar de weg zoals die in de wet beschreven

staat, zo veel mogelijk achterwege te laten en te focussen op de vragen waarin echt wordt gevraagd naar de implementatie, of deze wet voldoet en of we daar verandering in willen hebben. Dit kan betekenen dat u aan het einde uw lijstje afkruist en zegt: ik heb nog 45 vragen waarop ik geen direct antwoord heb gehad. Die kunnen we dan ook allemaal langslopen, maar dan krijgen we misschien een herhaling van zetten daarin. Ik markeer dit alleen even aan het begin omdat dit best een uitzonderlijke hoeveelheid is, ook voor mij, in wetsbehandelingen. Ik wil even bij u toetsen hoe ik dat in ieder geval wil aanvliegen. Dan kijken we wel hoe dat u bevalt, of niet.

De **voorzitter**:

Het is in ieder geval goed dat u deze bijsluiter geeft, want we hebben inderdaad tot 16.00 uur. Dat is een redelijk harde deadline, hoewel het natuurlijk uiteindelijk aan ons is hoelang het gaat duren. Maar het is een goede bijsluiter. Ik denk dat het in ieder geval goed is -- ik zie namelijk verschillende mapjes en dan zijn er vaak ook verschillende blokjes -- dat we steeds het hele blok afwachten en dan pas de vragen doen en kijken of er nog iets mist. Dan kunnen we helemaal aan het einde even inventariseren of Kamerleden nog vragen hebben openstaan. Mochten er Kamerleden zijn die nog 45 vragen open hebben staan, dan kunnen we misschien even kijken of we een deel bijvoorbeeld schriftelijk doen. Dan gaan we het zo doen. Ik zou even iedereen vriendelijk willen verzoeken om in ieder geval kort te zijn in de interrupties. Als je toch een interruptie pleegt, stel dan een korte vraag, want dan kunnen we zo veel mogelijk meters met elkaar maken. Het woord is aan de minister.

Minister **Van Weel**:

Dank, voorzitter. Ik heb zo meteen een korte inleiding. Dan doe ik de algemene vragen en de reikwijdte van de beide wetten. Dan kom ik op de meld- en zorgplicht. Daar waren een hoop vragen over. Dan ga ik in op het toezicht. Ook daar waren een hoop vragen over. Vervolgens ga ik in op de actualiteit, waaronder bijvoorbeeld Odido. Bij de artikelen over het weren van leveranciers wil ik even apart stilstaan. En dan heb ik nog een mapje overig, alvorens ik kom bij Caribisch Nederland en de aparte vragen die echt ingaan op de Cbw en de aparte vragen die echt ingaan op de Wwke. Ten slotte wil ik aan het einde van mijn termijn in ieder geval de ingediende amendementen alvast van een appreciatie voorzien.

Voorzitter. Vandaag staan twee belangrijke wetsvoorstellen centraal: het wetsvoorstel voor de Cyberbeveiligingswet en het wetsvoorstel voor de Wet weerbaarheid kritieke entiteiten. Allereerst dank dat we deze twee wetsvoorstellen gezamenlijk kunnen behandelen in één debat, want ze hangen nauw met elkaar samen. Het is belangrijk dat ze niet uit elkaar gaan

lopen, zowel wat betreft de inhoud, maar ook wat betreft het proces. Ze regelen belangrijke onderwerpen, namelijk de weerbaarheid en de digitale veiligheid van bedrijven en organisaties die essentiële diensten verlenen. Ze zijn ook hard nodig, want de Nederlandse vitale infrastructuur en onze digitale processen worden steeds vaker geconfronteerd met een stapeling van dreigingen. Door toegenomen geopolitieke spanningen zijn onze vitale infrastructuur en digitale processen steeds vaker doelwit van aanvallen door statelijke actoren, cybercriminelen en andere kwaadwillenden. Dit kan leiden en heeft al geleid tot verstoring of uitval van belangrijke processen.

De continuïteit van onze vitale en digitale processen is essentieel voor het goed functioneren van onze maatschappij; meerderen van u hebben daar al aan gerefereerd. Grootschalige verstoring of uitval daarvan raakt onze samenleving, onze economie en onze nationale veiligheid. Deze onderwerpen leven dan ook bij de inwoners van ons land. Dat zien we ook in de laatste Risico- en Crisisbarometer, het publieksonderzoek van de NCTV naar de beleving van de inwoners van Nederland van risico's en dreigingen. Daaruit blijkt dat meer dan de helft van de inwoners zich zorgen maakt over cyberdreigingen en het stoppen van vitale processen. De risico's voor de vitale infrastructuur zien we niet alleen in Nederland. We zagen vorig jaar ook een grote sabotage op Poolse spoorlijnen en begin dit jaar zaten heel veel huishoudens en bedrijven in Berlijn dagenlang zonder stroom, internet of verwarming. Ook dat kwam toen door een sabotageactie. De uitval en verstoring van vitale infrastructuur en digitale processen houdt dus niet op bij onze grens. Daarom ben ik blij, zeg ik ook in antwoord op een interruptiedebat dat u onderling had, dat we hier een Europese NIS2-richtlijn en een CER-richtlijn hebben, die in Nederland worden geïmplementeerd in de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten.

Voor bedrijven en organisaties die onder de wetten komen te vallen, geldt straks een wettelijke verplichting om maatregelen te nemen voor hun weerbaarheid en de beveiliging van hun netwerk- en informatiesystemen. Ook moeten zij grote incidenten melden. De impact van die wetsvoorstellen is aanzienlijk. Daarom heb ik de omzetting van de richtlijnen zorgvuldig aangepakt. Ondertussen hebben we, samen met de andere betrokken ministeries, bedrijven en organisaties, uitdrukkelijk opgeroepen om alvast aan de slag te gaan met de komst van beide wetten. De risico's die de bedrijven en de organisaties lopen, zijn er immers ook nu al.

Tot slot dank voor de vragen die u heeft gesteld, maar daar hadden we het al even over.

De **voorzitter**:

Alle 230.

Minister **Van Weel**:

Ik zal nu overgaan tot de beantwoording en begin met het kopje algemeen. Hoe wordt Nederland weerbaarder en veiliger van deze wetten en wat gaan burgers hiervan merken? Dat was een vraag van mevrouw Kathmann. Wat gaan ook de betrokken entiteiten merken van deze nieuwe wet? Als we kijken naar deze twee wetten, dan is het doel van de Cyberbeveiligingswet echt om de digitale weerbaarheid van Nederland te vergroten. Met deze wet komt er een zorgplicht voor een groot aantal organisaties en bedrijven die onder die wet gaan vallen. Ze moeten maatregelen nemen om de risico's van de beveiliging van hun netwerk- en informatiesystemen te beheren. Ze krijgen ook een meldplicht of, met andere woorden, de verplichting om grote incidenten te melden bij de daarvoor aangewezen instanties. Daarop vindt ook toezicht plaats. Langs die lijnen zal ik ook zo meteen ook de wetten behandelen, want dat zijn de kernelementen daaruit.

Als het gaat om de Wet weerbaarheid kritieke entiteiten gaat het, zoals gezegd, om kritieke entiteiten voor het doorgaan van processen in ons land. Dat gaat breder dan alleen cyber. Dat is niet helemaal nieuw. Er werd al gewezen op de Aanpak vitaal die al een aantal jaren loopt binnen mijn departement. Een hoop van die vitale aanbieders gaan nu naadloos op in de kritieke entiteiten zoals we die in de Wet weerbaarheid kritieke entiteiten zien. Een aantal leden vroeg ook wat er dan voor hen verandert. Onder andere dat nu een aantal dingen wettelijk geregeld worden. Dat geldt dus ook weer voor die zorgplicht, die meldplicht en dat toezicht. Voor diegenen die daar niet onder vallen, loopt de Aanpak vitaal gewoon door zoals die al deed. Voor de entiteiten die onder de Wwke komen te vallen, is de Wwke hun nieuwe Aanpak vitaal. Ik denk dat we gezorgd hebben dat beide implementaties naadloos op elkaar aansluiten.

Ook de Cyberbeveiligingswet komt niet uit het niets. We hadden al de Wet beveiliging netwerk- en informatiesystemen. Daar bouwt de Cyberbeveiligingswet op voort. Maar het grootste verschil is denk ik dat het aantal sectoren en het aantal entiteiten dat eronder valt, enorm is uitgebreid. Het aantal van 8.100 werd al genoemd. Ik kom later terug op de onderbouwing van die schatting.

Herkent de minister de kritiek op de uitwerking van de wetten? Uiteraard niet, zou ik zeggen tegen mevrouw Kathmann. Dat meen ik oprecht. Dit zijn hele omvangrijke wetten en ik denk dat daar ook de voornaamste reden in zit voor de vertraging die we hebben gezien in de implementatie. Zonder te willen wijzen denk ik dat een aantal landen hebben gemeld dat zij deze wet geïmplementeerd hebben, waarbij je je vervolgens kan afvragen of alles wat daaronder zit aan uitvoering, aan toezicht, aan systemen, aan de registratie van bedrijven, dan allemaal al gebeurd is. Daar kun je grote vraagtekens bij zetten. Nogmaals, ik zal geen namen noemen. Wij hebben ervoor gekozen om dat op een hele degelijke manier te doen. Met andere woorden, wij willen ook zeker weten dat we uiteindelijk een wet van kracht laten gaan, die ook

kan rekenen op systemen die werken, op bedrijven die weten wat ze moeten doen, dat er loketten zijn waar mensen heen kunnen gaan, dat toezichthouders met elkaar samenwerken. Ook daar komen we natuurlijk op te spreken. Dat heeft tijd gekost.

We hebben ook geprobeerd om zo veel mogelijk bedrijven en organisaties te benaderen, want ja, bedrijven moeten zelf die zelftoets doen, maar dan moeten we natuurlijk wel zorgen dat wij onze plicht hebben gedaan door te zorgen dat dat zo veel mogelijk bekend is. Er zijn brochures, flyers, nieuwsbrieven, webinars, vakbladen en Q&A's op alle websites ingezet. Daarmee hebben we geprobeerd om daar invulling aan te geven.

Dan zijn we nog niet klaar. Een hoop van u refereerden er al aan; er zijn echt een hoop zaken die nog nader moeten uitgewerkt in ministeriële regelingen of AMvB's. Ik denk dat we ook daarmee op schema liggen. Het is natuurlijk ook geen vreemde methodiek; we kennen het van wetten dat je zaken erna uitwerkt in onderliggende en lagere regelgeving.

We komen zo specifiek nog even te spreken over de leverantie-interventies en waar die dan mogelijk thuishoren; daar is ook een amendement over ingediend. In de kern is dat denk ik wel hoe wetten uitvoerbaar blijven. Dat zeg ik ook in reactie op de vraag van de heer Van den Berg of je een hoop van die zaken niet naar een hoger niveau van wetgeving zou willen hebben. Nogmaals, tijd is niet de bepalende factor geweest in het wel of niet opnemen van dingen in de wet. Dat is voornamelijk het niveau waarvan wij vinden dat iets erop thuishoort, maar ten tweede ook de veranderlijkheid van zaken.

De zaken die het snelst veranderen, wil je niet in de wet zelf geregeld hebben; een aantal van u refereerden daar al aan. Je wil die juist in een AMvB geregeld hebben, want je wil dat die wet in principe gewoon de komende tien, vijftien jaar door kan. Als je je realiseert dat die technologische veranderingen heel snel gaan -- kwantum werd al genoemd -- dan wil je dus een wet hebben die het raamwerk creëert waarbinnen je ook daarop kan anticiperen, maar wil je de ruimte houden om in een AMvB, zo'n ministeriële regeling, heel snel in te kunnen spelen op zaken die zich daarbij voordoen. Dan kan ik me voorstellen -- want dat kunnen heel relevante ontwikkelingen zijn -- dat de Kamer zegt: daar willen we dan wel bij betrokken zijn, daar willen we ook wat van vinden. In die zin heeft een aantal van u ook aandacht gevraagd voor de voorhang van AMvB's of wijzigingen die op deze wet of in ministeriële regelingen komen. Daar kan ik mij alles bij voorstellen, dus dat zult u zo in de appreciatie ook van mij horen. Ik denk dat dat het samenspel is tussen kabinet en parlement: om hier een weg in te vinden waarmee we wel die snelheid kunnen creëren waar die nodig is, maar de zorgvuldigheid en de politieke toets kunnen behouden waar die gewenst is en nodig is.

Kan ik een schriftelijk overzicht geven van wanneer ik verwacht dat alle hiervoor genoemde punten duidelijk zijn uitgewerkt? Ja, dat wil ik doen, want we weten welke stappen er gezet moeten worden. Aan sommige kan ik een

datum hangen en aan andere nog niet, want ik ben ook afhankelijk van collega-ministers. Maar dat is geen punt. Ik kan wat betreft een aantal punten wel toelichten waar we op dit moment staan. Van de AMvB's weet u inmiddels; die zijn er voor beide wetten. Bedrijven en organisaties kunnen zich op dit moment al registreren en kunnen ook al een melding doen. Ze hebben nu al een CSIRT en een toezichthouder. Daarmee kunnen de bedrijven ook nu al aan de slag conform de wet, maar het behoeft nog wel nader beleidswerk aan de uitvoeringsafspraken. Daarmee proberen we nou juist zo veel mogelijk aan te sluiten bij bestaande processen.

Een ander punt dat velen van u terecht hebben aangekaart, is de regeldruk. Hoe houden we de regeldruk, zeker voor bedrijven, zo laag mogelijk? Dat is onder andere door aan te sluiten bij toezichthouders die ze al hebben, en niet bij een nieuwe toezichthouder, zodat de sectoren in ieder geval al bekend zijn met de toezichthouder en vice versa. Dat doen we bijvoorbeeld ook -- ik kom zo nog terug op de gemeenten -- door aan te sluiten bij nu al bestaande processen of nu al gestelde eisen, zoals de BIO-eisen, waar gemeenten nu al aan voldoen. Het is wat dat betreft een beetje zoeken. Het verschilt ook per sector hoever men is, wat men aan middelen heeft en wat de makkelijkste manier is voor sectoren, bedrijven en overheidsorganisaties om te voldoen aan de plichten uit deze twee wetten. Dat is dan ook meteen de vaagheid die sommigen van u daar nog in lezen. Hoe ga je dat exact invullen? Liefst op een manier die zo veel mogelijk aansluit bij de behoeften van de sector, maar die er wel voor zorgt dat de waarborgen uit de wet worden gehanteerd. Dat betekent dat de zorgplicht nog niet in beton is gegoten. Als we die nu namelijk in beton zouden gieten voor elk bedrijf en elke organisatie, groot of klein, in welke branche dan ook, dan lopen we het risico dat we dingen zwaarder optuigen of onnodig bureaucratischer maken dan ze hoeven te zijn.

Nogmaals, de beginselen zitten hierin, maar daarom hecht ik er ook aan dat er vanuit de vakministers ministeriële regelingen komen voor het domein waarvoor zij verantwoordelijk zijn, omdat je dan ook kunt inzetten op die dingen doen waar het nodig is. Ik kom daar zo wat betreft onderwijs nog op terug, want dat is, denk ik, een heel aansprekend voorbeeld van hoe je daar maatwerk moet kunnen leveren. Daar komt nog bij dat we uit regeldrukonderzoeken en het mkb-panel rondom deze wet teruggekregen hebben dat bedrijven zich vaak al bewust zijn van de rol die ze hebben en die ze ook moeten spelen onder deze wet. Wat dat betreft is cybersecurity de afgelopen tien jaar natuurlijk ook binnen de boardrooms en de directies van bedrijven een steeds belangrijker onderwerp geworden. Deze wet komt dus niet uit het niets vallen.

Dan is er de vraag of deze wetten begrijpelijk en proportioneel zijn, en in hoeverre er een nationale kop op zit. Het antwoord op het tweede is, heel kort gezegd, "nee". We implementeren hiermee de NIS2-richtlijn en we implementeren hiermee de CER-richtlijn. Het enige wat wij doen, is gebruikmaken van sommige mogelijkheden die de wetten bieden om op nationaal niveau bepaalde sectoren bijvoorbeeld toch onder te brengen

binnen de reikwijdte van deze wet. Dit werd in uw inbreng "het keren en weren van water" genoemd. Keren en weren van water is in een hoop landen nice to have, maar ik denk dat het evident is dat het voor Nederland nou juist absoluut een kritiek element voor onze veiligheid is. U kunt zich voorstellen dat het verkrijgen van toegang in technische zin tot onze Deltawerken enorme gevaren kan opleveren voor onze gezondheid hier en voor ons land in den brede. Dit is waarom we onder andere die uitzondering hebben gemaakt.

Over het onderwijs ligt er de vraag of het niet met name gaat om specifieke kennisveiligheid binnen een deel van dat onderwijs. Moet je dan wel alles doen? Ik denk dat daar voor ons de vraag gestart is in hoeverre wij willen dat hogescholen hierbij komen te staan. Een aantal jaar geleden hebben we een hack gehad op een van onze hogescholen, met grote gevolgen destijds. Uiteindelijk is het de afweging geweest dat hogescholen al op een behoorlijk niveau van voldoen aan de Cyberbeveiligingswet zitten. Het wordt juist moeilijker om binnen die onderwijssector te gaan separeren tussen welke opleidingen wel en welke niet, welke instellingen wel en welke niet. De minister van OCW heeft er daarom voor gekozen, overigens in overleg met mij, om de volledige sector eronder te laten vallen. Zij krijgen wel meer tijd om hun eigen pad aan te brengen in hoe zij die zorg, die meldplicht, gaan inregelen.

Hoe kom je tot een essentiële entiteit, een belangrijke entiteit of een kritieke entiteit, vroeg mevrouw Kathmann. De Cyberbeveiligingswet kent twee categorieën: de essentiële en de belangrijke. Zoals ik altijd eindig met het kopje overige belangrijke vragen, is "belangrijk" de laagste categorie, maar wel nog steeds een relevante categorie in het kader van deze wet. In de bijlages bij de wet kun je specifiek zien welke sectoren vallen onder welke categorie. Binnen de Wet weerbaarheid kritieke entiteiten heb je dus de kritieke entiteiten. Een kritieke entiteit is automatisch ook een essentiële entiteit, maar het omgekeerde is niet per se het geval. Er zijn dus essentiële entiteiten die geen kritieke entiteit zijn voor het voortbestaan van de overheid, maar die vanuit cyberopzicht nog steeds wel een essentiële entiteit zijn.

De **voorzitter**:

Mevrouw Zwinkels, heeft u een vraag?

Mevrouw **Zwinkels** (CDA):

Volgens mij wilde u eventueel gemiste vragen per blokje doen. Toch, voorzitter? Maar kan een interruptie tussendoor wel?

De **voorzitter**:

Het is het handigst om alles, interrupties én vragen, aan het einde van het blokje te doen.

Mevrouw **Zwinkels** (CDA):

Prima. Dan wacht ik nog even.

De **voorzitter**:

Dus we maken eerst het hele blokje af. Er zijn namelijk zó veel vragen gesteld dat we hier anders vanavond nog zitten.

Mevrouw **Zwinkels** (CDA):

Ja, dat ben ik met u eens.

Minister **Van Weel**:

Dan de vraag over de AMvB's en in het verlengde daarvan de voorhang. Ja, er is een uitgebreide internetconsultatie geweest via de websites, onder andere die van de NCTV. Burgers en bedrijven hebben ook gereageerd op de AMvB's. We hebben die kritiek of suggesties ook meegenomen. Ik had het net al even over hoe we daar in de toekomst mee omgaan, met AMvB's en de rol van uw Kamer. Die internetconsultatie gaan we sowieso altijd doen. Dat spreekt voor zich. Dat geeft burgers, bedrijven en medeoverheden de gelegenheid om daarop te reageren. Mevrouw Kathmann heeft ook twee amendementen ingediend om een voorhangprocedure te regelen voor de uitwerking van de zorgplicht in de AMvB's. Daar sta ik positief in, vooral omdat die zien op toekomstige wijzigingen. We hoeven nu het proces dus niet om te keren, maar we moeten daar voor de toekomst wel rekening mee houden. Dit is nog niet mijn appreciatie, hoor, maar ik loop er wel een beetje op vooruit. Ik zie de griffier al kijken, van: hoe moet ik hiermee omgaan? Ik geef alleen een voorschot, dat mogelijk in de discussie kan helpen.

Kan ik schetsen wat er van entiteiten wordt verwacht in het eerste jaar nadat de wetten zijn aangenomen, en welke deadlines daarbij gelden? Dat was een vraag van mevrouw Kathmann. Alle bedrijven en organisaties die onder die wet vallen, moeten voldoen aan de zorgplicht. Dat is dus de verplichting om maatregelen te nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen. Daarnaast moeten ze voldoen aan de meldplicht. Nogmaals, de meldmogelijkheid is er nu al, maar de meldplicht wordt dan echt van kracht. Dat betekent dat je grote incidenten moet melden

bij de aangewezen instanties. Daar vindt in zijn geheel toezicht op plaats. Dat is de kern van wat er gebeurt op het moment dat deze wet van toepassing wordt. Die geldt vanaf dan dus ook voor alle organisaties.

Hoe helpen we die organisaties -- we kwamen zelf op een schatting van 8.100 -- om die weg te vinden? Weten ze dat dan wel? Wat kunnen we daar nog meer aan doen? Daar heeft de RDI een zelfevaluatietool voor gelanceerd. Gemeenten zijn aangewezen in de wet. Daarmee is het voor hen in ieder geval duidelijk dat zij hieronder zullen gaan vallen. Voor de gemeenschappelijke regelingen zijn gemeenten door het ministerie van Binnenlandse Zaken gevraagd om een validatie te doen of zij onder de Cbw vallen. Dat is gevraagd door middel van een brief. Bij vragen hebben we uiteraard nader contact met hen.

Vanwege het grote aantal entiteiten, met name de private, is het niet mogelijk om vanuit het Rijk voor iedere entiteit te bepalen of die onder de wet gaat vallen. In plaats daarvan is er juist zo veel mogelijk aan gedaan om ze met campagnes, Q&A's, websites en verwijzingen de juiste informatiepositie te geven om die beoordeling zelf te kunnen doen. Vervolgens kunnen organisaties, als ze die evaluatietool hebben doorlopen, zich gaan voorbereiden op wat dat betekent. Daarvoor hebben we stappenplannen aangeboden op de website van het NCSC, het Nationaal Cyber Security Centrum, en op de website van de NCTV. Er is geen inschatting gemaakt van de kosten. Dat is ook in het kader van de regeldruk. Het zijn ingeschatte gemiddelden. Per entiteit kan dat verschillen, bijvoorbeeld wanneer er juist tekortkomingen zijn in de digitale weerbaarheid die moeten worden gerectificeerd, terwijl bedrijven die eigenlijk al aan de hoge kant zitten wat betreft cyberbeveiliging wellicht juist geen kosten zullen hoeven maken. Het hangt er dus echt van af waar de organisatie staat.

De heer Van den Berg vroeg of er afzonderlijk wordt gestemd over het Cyberbeveiligingsbesluit en, zo ja, wanneer. Het is een AMvB, dus in die zin kent die geen parlementaire behandeling. Maar we hebben wel -- dat heb ik ook toegezegd voor het vervolg -- voor de zomer een concept voorgehangen, hier in de Kamer, om u daarin mee te nemen. In de verslagen over het wetsvoorstel hebben verschillende Tweede Kamerfracties gereageerd op dat concept, ook van de AMvB. Die reacties hebben we meegenomen in de nota naar aanleiding van het verslag. In die zin hebben we dus wel degelijk een wisseling van gedachten kunnen hebben, zij het niet in formele zin.

Waarom gaan we door na het negatieve advies van het Adviescollege toetsing regeldruk? Dat is vanwege het bijzondere karakter van deze twee wetten. Dat heeft te maken met het feit dat je het niveau van je cyberveiligheid landelijk niet op een hoger niveau kunt krijgen als je daarbij niet ook verplichtingen oplegt aan bedrijven en organisaties om hier iets mee te doen. Er werden al een aantal voorbeelden genoemd uit de actualiteit. Ik zal daar vanuit het kabinet niet per se een oordeel over hebben. Op dit moment gaan organisaties en bedrijven vrij divers om met hun

cyberbeveiliging. Het is gewoon noodzakelijk, juist vanwege de essentie van de services die ze bieden, voor ons als bevolking, zeg ik via de voorzitter tegen mevrouw Kathmann, dat daar een bepaald basisniveau is, zodat we geen incidenten hebben waarbij vitale processen in gevaar komen of we er achteraf achter komen dat er eigenlijk met de pet is gegooid naar de cyberbeveiliging. Dat is wat deze wetten doen. Dat kun je nou eenmaal niet doen door dat op een bepaalde manier toch in regels te vatten.

Dat brengt dus altijd iets van een last met zich mee, maar daar hebben we wel een aantal mitigerende maatregelen voor genomen. Ten eerste de proportionaliteit. Dat is echt een leidend principe geweest bij deze wetten. Daarom zijn ze ook risicogebaseerd. Iedere organisatie moet maatregelen nemen die passend zijn voor de organisatie zelf. Daarom is het maatwerk. Daarom zeg je soms: waarom is dit niet tot achter de komma uitgewerkt? Dat heeft dus ook te maken met het proberen te verminderen van die regeldruk. Zoals ik al eerder zei, komt in die regeldrukonderzoeken ook naar voren dat een hoop bedrijven zich eigenlijk wel realiseren dat ze hier wat te doen hebben en een rol in te spelen hebben. Het is dus niet per se zo dat deze wet voor een heleboel bedrijven die zich er al bewust van zijn, heel veel meer met zich meebrengt, want die opereren eigenlijk al via dat principe.

Kunnen we bij de invoeringstoets kijken naar de daadwerkelijke regeldruk? Dat is een vraag van de heer Van den Berg. De invoeringstoets is echt bedoeld om grote knelpunten zo snel mogelijk op te kunnen lossen, om ervoor te zorgen dat de wet alsnog ingevoerd kan worden. Ik wil daar echter wel naar gaan kijken bij de evaluatie. Laat ik de koe meteen bij de hoorns vatten. Een aantal van u heeft het daarover gehad en vindt vijf jaar te lang. Het helpt ons dat we enigszins verlaat zijn met de invoering van de wet, waardoor het punt waarop de Commissie met haar eerste evaluatie komt al dichterbij komt. Dat is volgend jaar al. Ik wil kijken of we spoedig na de evaluatie van de Commissie -- laten we zeggen: binnen twee jaar na invoering van de wet -- een evaluatie kunnen doen. Daar nemen we dan ook de regeldruk in mee.

Dat waren alweer zes vragen, denk ik, voorzitter.

Waarom wordt de verantwoordelijkheid voor de uitvoering ook bij de decentrale overheden neergelegd? De uitvoering van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten wordt niet bij decentrale overheden belegd. Er worden sectoren aangewezen die onder de wet vallen, en onder die sectoren vallen ook decentrale overheden. Het is dus niet iets wat zij als een service doen. Het is niet een taak die wij overhevelen van het Rijk naar gemeenten. Ik hoorde al iets over de knaken-en-takendiscussie. Nee, elke entiteit die wordt aangewezen onder deze twee wetten, zal daar zelf maatregelen op moeten nemen. Dat betreft dus ook gemeenten. In die zin volgt het dus een andere systematiek. We steunen de lokale overheden daar natuurlijk wel bij. Daar zijn voldoende middelen voor. We hebben dit overigens ook overlegd.

Dat brengt mij bij de UDO, de Uitvoerbaarheidstoets Decentrale Overheden. Die is ook hier gedaan. Dat is overigens geen document met een rapport en een stempel van de UDO-dienst. Nee, dat is een proces, waarin je samen met de lokale decentrale overheden bekijkt hoe we de wet daar op een zo goed mogelijke manier invoeren en tegen welke knelpunten we aan lopen. Die zijn dus ook meegenomen in de memorie van toelichting bij het wetsvoorstel en in de wijze van implementatie. Daar vindt u de uitkomsten daarvan terug.

De mkb-toets is een andere toets die vaak wordt gedaan. Er is een volwaardige mkb-toets uitgevoerd. Ik heb al gezegd dat regeldruk een belangrijk punt was voor de manier waarop we deze wet invoeren. Uit die mkb-toets bleek steun voor de risicogebaseerde aanpak, want dat is natuurlijk wat het uiteindelijk behapbaarder maakt.

Daarnaast is in de wet en in de omliggende besluiten verduidelijkt dat bijvoorbeeld de risicobeoordeling onder beide wetten zo veel mogelijk door bedrijven kan worden gecombineerd. Ze hoeven dus niet twee keer een risicobeoordeling te doen, maar één middel volstaat voor de verplichting onder beide wetten. Ook dat is een poging om die regeldruk naar beneden te brengen.

Dan nog meer over de samenhang tussen de fysieke en digitale weerbaarheid. Mevrouw Zwinkels vroeg hierover: hoe gaan we dat borgen? We behandelen tenslotte die wetten hier vandaag samen. Dat heeft zijn reden. Ze zijn in samenhang door ons opgesteld. Dat geldt ook voor de Europese richtlijnen waarvan ze afgeleid zijn. Om dat in de praktijk te borgen, werken we dus aan de inrichting van één meldpunt voor beide wetten. Dat meldportaal zal door het Nationaal Cyber Security Centrum worden beheerd. Ik zei net al dat de risicobeoordeling van beide wetten door bedrijven die onder beide vallen ook gezamenlijk kan worden gedaan, waardoor die in ieder geval niet twee keer een risicobeoordeling hoeven op te stellen en alle dreigingen in één keer meegenomen kunnen worden.

Dan nog even over die evaluatie. Mevrouw Kathmann en meneer Van den Berg vroegen: als we in die evaluatie zaken toch liever in de hogere wetgeving zouden willen hebben, staan we daar dan ook voor open? Ja, uiteraard. Ik denk dat de evaluatie dat ons ook moet geven. Nogmaals, ik vind niet dat we er ons hierbij met een jantje-van-leiden van af hebben gemaakt. Er zit echt een gedachte achter: wat staat er wel in die wet en wat zit er in lagere regelgeving? Als uit de evaluatie blijkt dat je dat beter anders kunt doen, zullen we dat te zijner tijd natuurlijk niet nalaten.

Misschien moet ik het nog even hebben over decentrale overheden. Ook de provincies werden nog genoemd. Wat ons betreft is er nog geen noodzaak tot algemene compensatie van medeoverheden voor de implementatie van deze wet, omdat in de praktijk een hoop van die verplichtingen al van toepassing zijn op dat niveau. Ik noemde al de BIO, maar ik kan nu ook zeggen waar dat ook alweer voor staat. Dat is de Baseline Informatiebeveiliging Overheid. Ook voor de meldplichtcriteria is aangesloten bij hetgeen zij al moesten doen. Die

meldplicht gold namelijk al voor hen. We hebben daarin geen wijzigingen aangebracht in deze wet. Er zijn marginale extra verplichtingen voor decentrale overheden, zoals de registratieplicht en de trainingsplicht voor bestuurders. Die werd ook al door enkelen aangehaald. Naar verwachting zijn de financiële gevolgen voor de medeoverheden daarmee beperkt. BZK, Binnenlandse Zaken, bekijkt samen met de medeoverheden hoe ze kunnen worden ondersteund. Dat geldt natuurlijk met name voor de kleinere organisaties. Denk bijvoorbeeld aan gezamenlijk opleidingen volgen, waardoor gemeenten dat niet allemaal afzonderlijk hoeven in te vullen.

In dit blokje heb ik nog de antwoorden op twee vragen, voorzitter. Waarom is er een verschil in bewaartermijnen? Heb ik trouwens niet een apart kopje AVG? Nee. Oké, dan behandel ik deze vraag nu. Waarom is het verschil in bewaartermijn tussen die CSIRT's, de Cyber Security Incident Response Teams, en de toezichthouders zo groot? Dat heeft te maken met de andere taakopvatting die ze hebben. Voor de CSIRT's gaat het, op het moment dat zij een melding krijgen, om helpen bij het oplossen van het probleem dat er is, om andere organisaties te informeren en zo hopelijk verdere uitbreiding van de problemen te voorkomen, en om daarvoor de contacten te leggen die nodig zijn, bijvoorbeeld met andere partijen die zouden kunnen ondersteunen. Dat is allemaal gericht op het hier en nu. Dat is wat CSIRT's doen en wat ze het leukste vinden. Die zitten niet in archiefkasten te neuzelen naar het verleden. Dat moeten toezichthouders natuurlijk af en toe wel doen, omdat die uiteindelijk bestuurlijke dwangmiddelen moeten kunnen inzetten. Je kunt je beroepsprocedures, boetes et cetera voorstellen. Denk aan de meest zware variant, waarin een bestuurder persoonlijk aansprakelijk wordt gesteld. Dat kunnen zaken zijn die rustig een paar jaar voortduren. Daarom moet de toezichthouder wel over ruimere middelen kunnen beschikken dan de korte bewaartermijn die we wel graag voor die CSIRT's willen hanteren.

Dan weer een heel ander onderwerp. Kan ik er al iets over zeggen hoe vaak de bestaande hulptools zijn gebruikt door bedrijven en entiteiten? We zien dat ze in toenemende mate worden gebruikt en dat die actieve mediacampagne daar ook wel bij helpt. De eerste stap is checken of bedrijven onder de Cyberbeveiligingswet gaan vallen. De zelfevaluatietool waarmee je dat kunt doen, is tot nu toe meer dan 205.000 keer geraadpleegd. Dat is wel echt heel veel. Dat is een positieve stap. Steeds meer organisaties gaan na die eerste stap ook naar de website van het Nationaal Cyber Security Centrum om de daar beschikbare middelen en tools te gaan gebruiken. Ik denk dat dat een goede eerste stap is. De quickscan tool waarmee organisaties inzicht krijgen in hoe de cyberbeveiliging van een organisatie ervoor staat, is 31.000 keer doorlopen. 6.100 organisaties hebben de scan volledig ingevuld. Van oudsher draagt het Nationaal Cyber Security Centrum de hulptools, handleidingen en infosheets actief uit via relatiebeheerders. Sinds vorig jaar zetten ze ook onlinewebinars op om de hulptools et cetera op grotere schaal toe te lichten. Per webinar zien we dat

er meer dan 1.500 organisaties deelnemen. Ook dat is dus echt aanzienlijk. De LinkedInpagina van het NCSC -- je telt niet mee als je die niet hebt -- heeft inmiddels 70.000 volgers. Die volgen dus ook de wekelijkse posts over de Cyberbeveiligingswet. In die zin denk ik dat de outreach een geslaagd onderdeel is geweest van deze wet en dat het met de bekendheid echt wel goed zit.

Dat was mijn eerste blokje.

De **voorzitter**:

Als ik het goed heb, was dit het blokje reikwijdte. We gaan dus nog naar zorgplicht en toezicht; dat komt er allemaal nog aan. Dit was het blokje reikwijdte. Ik kijk even naar links om te zien of mensen vinden dat er nog vragen zijn blijven liggen.

Mevrouw **Zwinkels** (CDA):

Ik had eigenlijk één interruptie naar aanleiding van een antwoord. Ik ben blij met de antwoorden ten aanzien van kleinere gemeenten. Dat is goed om te horen. Ook ten aanzien van de coördinatie werden er al wat punten aangehaald. Maar ik maak me toch wel zorgen over de onderwijssector. Het antwoord was "de hele sector valt er gewoon onder", maar we hebben juist proportionaliteit hoog in het vaandel staan en we willen juist dat het risicogebaseerd is. Dat zie ik niet helemaal terugkomen als het gaat om de reikwijdte voor het onderwijs. Ik wil dus toch graag aan de minister vragen of hij ons er op de een of andere manier over gerust kan stellen dat er ook wordt getracht om proportionaliteit te borgen richting het onderwijs.

Minister **Van Weel**:

Zeker, maar wat betreft proportionaliteit lopen we ook juridisch tegen een aantal begrenzingen aan. Daar zullen we nog over komen te spreken in een ander format als het gaat over kennisveiligheid. Het is ontzettend moeilijk om te bepalen welk deel van een onderwijssector nou onder een ander regime moet vallen dan het overige deel van een onderwijssector. Dat is juridisch moeilijk, dat ligt bij bonden moeilijk en dat is ook in de uitvoering niet altijd makkelijk, omdat je het ook kunt hebben over delen binnen één onderwijsorganisatie. Daar zou je dan verschillende regimes op van toepassing moeten verklaren en dan vallen bestuurders deels wel onder de Cyberbeveiligingswet en deels niet. Dat is dus echt heel complex. Daarom heeft de minister van Onderwijs gezegd: we hebben al de organisatie van onze eigen CSIRT's -- "SURFcert" heet dat binnen de onderwijssector -- die nu al de volledige sector bedient, dus laten we dan ook de volledige sector naar datzelfde niveau brengen. Ook dat is deels proportionaliteit: ervoor zorgen

dat je het niet complexer maakt voor de sector door ze eronder te brengen, terwijl je vanuit de inhoud zou zeggen dat het grootste risico natuurlijk ligt bij sommige delen van die sector. Dat ben ik helemaal met u eens.

Mevrouw **Zwinkels** (CDA):

Tot slot op dit punt. Dit antwoord stelt mij al iets meer gerust. De minister gaf ook aan: we geven het onderwijs wat meer tijd; het tijdpad is wat ruimer. Kan er dan worden toegezegd dat op die manier samen met het onderwijs, met SURF en andere partijen die al veel inspanningen hebben verricht, kan worden gekeken wat prioriteit krijgt, wat we eerst doen en wat ook later kan?

Minister **Van Weel**:

Zeker. Dat zeg ik mede namens de minister van Onderwijs. Ik wil, zeg ik in algemene zin, namelijk zeker niet de algemeen verantwoordelijke worden voor alle sectoren. Ik was juist erg blij dat dat risico in ieder geval in de wet gespreid is. Zij zal dat dus doen. Zoals gezegd hebben ze 36 maanden om te voldoen aan de verplichtingen vanuit de wet. Die zullen worden benut om dat op een verantwoorde en proportionele manier te doen.

De heer **Van den Berg** (JA21):

Een vervolgvraag na mevrouw Zwinkels van het CDA. Wij hebben een amendement in voorbereiding dat eigenlijk het volgende stelt. Je hebt de hele sector qua hoger onderwijs. De NIS2-richtlijn laat expliciet de ruimte om ervoor te kiezen om instellingen al dan niet onder de wet te brengen. We zouden, denk ik, een lid kunnen toevoegen dat zegt: "het hoger onderwijs en het wetenschappelijk onderzoek die kritieke onderzoeksactiviteiten verrichten". Volgens mij is het best proportioneel om in te schatten of hogescholen het wel of niet doen en die instellingen zodoende wel of niet onder de wet te brengen. Kortom, doen we dat niet, dan krijgen we overbodige regeldruk. Hoe kijkt de minister daarnaar?

Minister **Van Weel**:

Ik schetste het net al even, meneer Van den Berg. U zegt namelijk: "de instellingen die". Onder de woorden die u daarna kiest, gaat een hele wereld schuil. Die zul je dan namelijk in wetgeving moeten definiëren; die zul je verder moeten uitwerken. Dan loop je tegen hele complexe zaken aan. Wanneer is iets nou kritisch, zeker waar het gaat om kennisoverdracht? Er zijn een aantal voorbeelden uit het verleden waarbij het wél tot mogelijkheden heeft geleid -- denk aan het weren van bepaalde studenten bij opleidingen tot kernfysicus -- maar in bredere zin is het voor iets als

informatica of lucht- en ruimtevaart ontzettend moeilijk om te doen. Je loopt namelijk al heel snel aan tegen ofwel discriminatie ofwel selectiviteit ofwel de inhoudelijke afweging om onderscheid te maken tussen instellingen, vandaar dat ik zeg: die weg leek ook de minister van Onderwijs niet begaanbaar voor dit doeleinde. Bovendien vallen ze al binnen één cyberbeveiligingsregime. Je zou dus ook meer druk creëren door het weer op te knippen, vandaar de keuze om het toch in zijn geheel te doen.

De heer **Van den Berg** (JA21):

Dan zou het in de praktijk dus zo zijn -- dat zeg ik niet alleen omdat ik zelf christen ben -- dat de hogeschool voor theologie ook onder deze wet zou vallen. Ik durf met zekerheid te stellen dat die geen kritieke onderzoeksactiviteiten verricht in het kader van deze wet. Ik hoor dat het een stuk moeilijker zou zijn. Is de minister het desondanks met me eens dat de uitkomst is dat hogescholen die hier niks mee te maken hebben, toch moeten rapporteren, met de bijkomende lastendruk?

Minister **Van Weel**:

Eén. Het kan een faculteit theologie zijn binnen een universiteit die wel interessante vakgebieden heeft. Die hebben dan één ICT-systeem. Er zijn zelfs meerdere hogescholen die gezamenlijk één IT-organisatie hebben. Daar ga je dan dus alweer in knippen. Bovendien is de gevoelige informatie niet alleen de inhoudelijke informatie. Die moet je beschermen. Soms kun je het op inhoud ook wat verder aanscherpen. Maar het gaat hier ook om de algemene cybersecurity. Ook de persoonsgegevens van studenten zijn al interessante informatie voor criminelen. Dat hebben we met de Odidohack gezien. Ik noem ook het überhaupt op zwart kunnen zetten van een systeem. Theologiestudenten willen op een gegeven moment afstuderen. Dan moet er wel een systeem beschikbaar zijn. Ik snap de kennisveiligheidsroute, maar ik denk dat het in praktische zin toch makkelijker is om de sector als geheel aan te wijzen.

De **voorzitter**:

Ik kijk even naar de minister. Daarnet werden de bewaartermijnen al even aangeraakt. Was dit ook het blokje over de bewaartermijnen?

Minister **Van Weel**:

Ik heb best een goed geheugen, maar ... Ik heb ze alle 233 gelezen, maar ik weet niet ... Die vragen komen bij het blokje overig, hoor ik van mijn ondersteuning. Gelukkig heb ik een extern geheugen!

De **voorzitter**:

O, het kwam heel even voorbij, maar dan wacht ik daarop. Dan is het woord weer aan de minister voor het volgende blok. O, de heer Van den Berg heeft nog een vraag.

De heer **Van den Berg** (JA21):

Het waren inderdaad een hoop vragen, dus ook ik moest het overzicht weer even zoeken. Als ik het goed hoorde, gaf de minister dus eigenlijk aan dat er inderdaad de facto twee jaar na invoering van de wet een eerste evaluatie komt. Hoe zit het dan met een terugkerende evaluatie? Bij de Wet weerbaarheid kritieke entiteiten is zo'n evaluatie helemaal niet voorzien en bij de Cyberbeveiligingswet staat die, als ik het goed zeg, op drie jaar doorlopend. Of is het vijf jaar? Nu begin ik zelf ook te twijfelen. Maar hoe kijkt de minister ernaar dat die evaluatie bij de Wet weerbaarheid kritieke entiteiten in zijn geheel ontbreekt?

Minister **Van Weel**:

Je hoeft niet alle wetten continu te evalueren. Wat mij betreft is het geen uitgangspunt dat je continu evaluaties hebt. Dat is natuurlijk wel van belang als je iets invoert, want dan wil je gewoon op enige termijn kunnen constateren of de wet haar werk heeft gedaan, wat ermee gebeurd is, hoeveel keer er boetes zijn uitgedeeld en of dat heeft geleid tot een veranderend beeld. Ik denk dat de cyberwereld wat dat betreft dusdanig fluïde is dat die driejaarlijkse terugkerende evaluatie, dus na 36 maanden, heel nuttig kan zijn. Ik zie dat nut op voorhand niet per se bij de Wwke. Als je dit systeem hebt ingeregeld, is het verder in principe een redelijk stabiel beeld, want we weten wat die kritieke entiteiten zijn. Ik denk dat dat het onderscheid is tussen die twee werelden. Dat wil niet zeggen dat er verder niks gebeurt wat betreft de aanscherping van beleid.

De heer **Van den Berg** (JA21):

Exact. Dat ben ik met de minister eens. Maar we hebben hier te maken hebben met een best wel verregaande samenhang tussen de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. Het werd net al genoemd: als je een kritieke entiteit bent, dan ben je tegelijkertijd ook een essentiële instelling in het kader van de Cbw. Als er dus nuttige punten, punten van verbetering, uit die evaluaties komen, ziet de minister dan een andere manier om die ook in de Wet weerbaarheid kritieke entiteiten mee te nemen, zodat dat wel synchroon blijft? Kan hij dat toezeggen?

Minister **Van Weel**:

Ja, dat lijkt me werkbaar. Dan zou je bekijken wat de implicaties zijn van het meenemen van de uitkomsten van de evaluatie van de Cyberbeveiligingswet, die je elke drie jaar doet, op de Wwke. Dat is een lightvorm van evalueren, maar dan blijven die twee inderdaad wel gelijklopen. Wat betreft de leveranciersclausule -- ik bedenk maar wat, hoor -- zou je bijvoorbeeld niet willen dat dat uit elkaar gaat lopen.

De heer **Van den Berg** (JA21):

Ik ga het overwegen. Dank u wel.

De **voorzitter**:

De minister kan verder met het volgende blok.

Minister **Van Weel**:

Dat blok gaat over de meld- en zorgplicht. Een waren een hoop vragen over of we kunnen komen tot één meldloket. Ik lichtte net al een tipje van de sluier op: ja, dat gaan we op een lastenluwe manier inrichten; we gaan dat bundelen in één meldpunt. Dat meldpunt komt bij het Nationaal Cyber Security Centrum. Zowel voor de Cyberbeveiligingswet-meldingen als voor de Wwke-meldingen komt er dus één loket. Daarnaast kan dit meldpunt ook worden gebruikt voor meldingen op basis van de Digital Operational Resilience Act voor de financiële sector, en de netcode voor de elektriciteitssector. In die zin vangen we dus nog twee andere richtlijnen en verordeningen onder dat ene meldpunt. We gaan ook kijken of het haalbaar en uitvoerbaar is om voor andere cybermeldingen een nationaal meldloket in te richten, voor meerdere wetgevende kaders. Dat gebeurt dus buiten de Cyberbeveiligingswet om. Dat onderzoek loopt nog.

Hoe worden bestuurders geïnformeerd over alle stappen die zij moeten nemen? Bestuurders en CISO's zijn in de communicatie die ik net al noemde de belangrijkste doelgroepen die wij proberen te bereiken. Die communicatie loopt ook actief. Ik heb net een aantal van de middelen daarvoor toegelicht, waaronder de webinars. Ze worden niet alleen geïnformeerd, maar ook ondersteund bij het nemen van de nodige stappen voor de meldplicht, de zorgplicht en de registratieplicht. Bij de Wwke werkt het nog wat directer. Daar worden de bestuurders gewoon direct benaderd door de verschillende vakdepartementen en dus vanuit de overheid.

De heer Van den Berg vroeg: hoe kun je rechtsongelijkheid voorkomen tussen sectoren bij de verschillende interpretaties van die zorgplicht? De Cyberbeveiligingswet en de Wwke maken het mogelijk om via ministeriële regelingen sectorspecifieke regels te maken voor de invulling van de zorgplichtmaatregelen. De vakministers hebben hier ook gebruik van gemaakt. Een groot deel van deze ministeriële regelingen zijn in november van het afgelopen jaar in consultatie gegaan. Het is uiteindelijk aan de toezichthouder om te beoordelen of de entiteit voldoende invulling heeft gegeven aan de zorgplichtmaatregelen. Die zal daarbij ook risicogebaseerd te werk gaan om rechtsongelijkheid te voorkomen.

Waarom mogen entiteiten zelf inschatten wat proportioneel en effectief is? Waarom zijn er geen heldere normen? Dit borduurt daar een beetje op voort. Dat gebeurt, weer, om die regeldruk zo veel mogelijk te vermijden. Dat hangt echt af van de risicoanalyse die ze zelf moeten gaan maken. Dat zal uiteindelijk de basis zijn voor de maatregelen die je dan neemt. Dat verschilt echt per entiteit. Door die ruimte te laten, doen we ook recht aan de sectorale verschillen die er zijn. We hadden het net al over de onderwijssector en over hoe je binnen één sector al verschillen kunt creëren. Bij die beoordeling kunnen ze gebruikmaken van bestaande normenkaders, zoals de ISO 27001 en verschillende hulpmiddelen vanuit de Rijksoverheid.

In dat verlengde stelde de heer Van den Berg ook vragen over termen als "kan" en "kunnen". Dat vloeit precies voort uit het feit dat we entiteiten de ruimte willen geven om op hun eigen manier invulling te geven aan die zorgplicht. De maatregelen en de evenredigheid daarvan kunnen per entiteit verschillen, vandaar de open normen. Maar de kaders zijn wel hetzelfde, namelijk de ISO-norm en datgene wat wij bieden vanuit de Rijksoverheid.

Hoe verhoudt de open norm van de zorgplicht zich tot hele hoge bestuurlijke boetes? Laten we eerlijk zijn: die hoge boetes zijn een eindstation en geen beginstation. Elke boete die uiteindelijk zal worden opgelegd, zal afgestemd worden op de ernst van de overtreding en de mate waarin die verwijtbaar is aan de entiteit. U kunt zich voorstellen dat alle rechtsbeginselen die gelden in ons algemeen bestuursrecht ook van toepassing zijn op deze wet. Dat zal echt betekenen dat niet altijd de maximale boete wordt opgelegd. Een boete zal altijd proportioneel moeten zijn en toetsbaar aan de normen die zijn neergelegd, in het bijzonder aan de ministeriële regelingen die uiteindelijk per sector komen. Er zijn ook heel veel best practices voorhanden, ook van het NCSC, waardoor entiteiten ongeveer weten wat er voor hen van toepassing is, wat ze mogen verwachten.

Ik weet niet of de dubbele beboeting nog terugkomt, maar dat kan überhaupt niet in het Nederlandse stelsel. Volgens de Algemene wet bestuursrecht kun je niet twee boetes opleggen voor hetzelfde delict, dus dat kan ook in dit geval niet voorkomen, zelfs al zouden verschillende toezichthouders daar op onverklaarbare wijze toe komen.

Hoe zit het met de verschillende toezichthouders en de mogelijke overlap daartussen? Gezegd is al dat we zo veel mogelijk aansluiten bij de toezichthouders die de organisaties en de entiteiten al kennen, juist omdat we dan niet weer een extra laag creëren en niet weer een extra rechtspersoon waarmee entiteiten zaken moeten doen. Die toezichthouders moeten elkaar vinden. Dat is essentieel en dat hoor ik ook terug in de vragen. Als dat niet goed gaat, krijg je dus wel overlap. In de praktijk vindt de samenwerking nu al plaats in het Samenwerkend Toezicht Digitale Weerbaarheid en het Directeurenoverleg Toezicht Digitale Weerbaarheid. Ze werken inderdaad aan toezichtprotocollen om dat voor iedereen duidelijk en transparant te maken en om toezichtlasten te voorkomen. De vraag was of we daarover kunnen communiceren als dat uiteindelijk tot wasdom is gekomen. Dat zullen we gaan doen.

Wat nou als grote organisaties uit meerdere entiteiten bestaan? Wanneer is groepsregistratiefunctionaliteit operationeel? Grote organisaties die uit meerdere entiteiten bestaan kunnen zich straks als groep registreren en dan kan ervoor gekozen worden om alle meldingen door één contactpersoon of één individu te laten verrichten namens de gehele groep. Die functionaliteit zal met ingang van 1 april operationeel worden, dus vanaf dat moment hebben we ook de groepsregistratie.

Hoe voorkom je dat je je op meerdere plekken moet registreren of dat er tegenstrijdig wordt geregistreerd? Dat was ook een vraag van de heer Van den Berg met betrekking tot de beide wetten. Er is slechts één meld- en registratieportaal waar alle bevoegde autoriteiten en de CSIRT's toegang toe krijgen voor zover dat relevant is voor hun werkzaamheden. Er zullen daarom geen meerdere of tegenstrijdige registraties zijn. Als een organisatie zich met haar unieke KvK-nummer registreert, dan kan deze niet nog een keer worden geregistreerd in hetzelfde systeem. Ook daar kan dus geen dubbeling in komen. De beschikbare informatie wordt door middel van eHerkenning bij de Kamer van Koophandel opgehaald. Bij overheden worden de gegevens daarvoor uit het Register van Overheidsorganisaties gehaald.

Voor de Wwke geldt geen registratieplicht, want die entiteiten worden aangewezen door de overheid. Mochten organisaties door meerdere departementen worden aangewezen, dan zal dit onderling moeten worden afgestemd. Bij het doen van een melding kan een organisatie aanvinken onder welke wet zij deze melden doet. Daarbij kunnen beide wetten worden aangevinkt. Dat geldt dus voor de meldplicht.

Hoe voorkomt een kabinet dat bestuurders in de problemen komen, omdat ze een meldtermijn hebben gemist. Dat was een vraag van mevrouw Martens. De meldplichttermijn moet natuurlijk gehaald worden. Daar zal de toezichthouder primair op toezien. Die zal de rechtspersoon daar ook op aanspreken. Ik durf het wel aan om te zeggen dat het schorsen van bestuurders vanwege het eerste missen van de meldplicht niet snel de eerste stap zal zijn die een toezichthouder daarin neemt. Dat is ook niet de manier

waarop toezichthouders omgaan met bestuurders. Dan is er wel wat meer aan de hand. Laat ik het zo zeggen.

Over moeder- en dochterondernemingen heb ik het al gehad. Dat gaat over de groepsmelding.

Ik denk dat ik daarmee aan het einde ben van de meld- en zorgplicht. Het volgende blokje is het blokje toezicht.

De **voorzitter**:

Dit was het blokje meld- en zorgplicht. Hierna volgt toezicht. Ik kijk even naar links. Zijn er nog Kamerleden die vragen hebben gemist? Ja, in ieder geval mevrouw Faber. Daarna mevrouw Zwinkels en de heer Van den Berg. Mevrouw Faber.

Mevrouw **Faber** (PVV):

Even ter verduidelijking: viel hier ook toezicht onder? Of komt dat nog later? O, dat komt nu. Dan houd ik nog even mijn mond.

Mevrouw **Zwinkels** (CDA):

Ik was net als mevrouw Faber even in de war, want het ging al veel over toezicht. Ik ga mijn vraag toch stellen, want de minister ging daar al op in. Mijn vraag gaat over het kunnen opleggen van twee boetes voor hetzelfde delict. Ik vroeg net vooral naar de overlap: meer toezichthouders kunnen zich geroepen voelen om een bedrijf of een andere organisatie tot de orde te roepen. Is straks ook vastgelegd welke toezichthouder voorrang krijgt? Ik ben daar toch wel benieuwd naar. Welke van de twee gaat dan daadwerkelijk een procedure starten, zodat zaken niet dubbel worden gedaan of naast elkaar lopen, nog los van wat uiteindelijk het oordeel zal zijn? Wat is het antwoord van de minister daarop?

De **voorzitter**:

Ik kijk ook even naar de minister. Valt dat misschien toch onder toezicht?

Minister **Van Weel**:

Ik heb het zelf een beetje uitgelokt door de toezichthouders al te noemen bij de meld- en zorgplicht. Op de eerste vraag: twee boetes voor hetzelfde kan niet. Twee toezichthouders voor één organisatie kan wel. Sommige organisaties vallen ook zonder deze wet al onder meerdere toezichthouders.

Bij de Cbw en de Wwke moeten de toezichthouders samenwerkingsafspraken gaan maken. Daarin moeten dit soort zaken en protocollen nou juist naar voren komen: als een overtreding van een van beide wetten wordt geconstateerd, welke toezichthouder handhaaft dan bij wat voor overtreding? Die samenwerkingsafspraken is men in het directeurenoverleg aan het uitwerken en wil men voor de invoering van de wet gereed hebben. Ik zei al dat ik daarover met uw Kamer wil communiceren als die er zijn, maar in principe moeten die aan de organisaties helderheid gaan geven.

De **voorzitter**:

Dan de heer Van den Berg. O, sorry, meneer Van den Berg. Mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Heel kort, voorzitter. Ik ben blij met die toezegging. Ik verwacht dat die al in april of iets dergelijks onze kant op kunnen komen, want net verwees de minister naar 1 april. Ik heb ook gevraagd welke rol de Rijksinspectie Digitale Infrastructuur nog eventueel kan spelen om die centrale regie wat meer op te pakken. Daar ben ik ook benieuwd naar.

Minister **Van Weel**:

Dat laatste doet ze. De datum van 1 april was gerelateerd aan de mogelijkheid om zich als groep te registreren als entiteit. Ik wil die 1 april dus niet per se ophangen aan de samenwerkingsafspraken. Of heb ik dat eerder wel gezegd? Nee, toch? Ik kijk even naar rechts. Nee. Maar die afspraken komen wel voor de invoering van de wet.

De **voorzitter**:

De minister zegt toe: voor de invoering van de wet. De heer Van den Berg.

De heer **Van den Berg** (JA21):

Wederom volgend op mevrouw Zwinkels: het is goed dat er onderling wordt gecoördineerd. Als ik het goed begrijp, is die onderlinge afstemming echter niet geborgd in de wet en volgens mij wordt van de onderlinge afspraken die gemaakt zullen worden, ook geen melding gedaan in de Staatscourant. Ik zou de minister willen vragen hoe hij daarnaar kijkt. Is het niet beter om die afspraken te borgen door die in de Staatscourant openbaar en transparant te maken? Hij onderkent zelf dat die belangrijk zijn.

Minister **Van Weel**:

Ik vrees dat dit niet met een schaartje te knippen is. Je zult moeilijk op wetsniveau kunnen vastleggen welke toezichthouder het voortouw heeft bij de implementatie van deze wetten. Bij vastleggen in de wet zou je dus niet verder komen dan het listen van alle toezichthouders die hierbij betrokken zijn, en dat heeft dan weer weinig toegevoegde waarde. Het ging immers juist om het creëren van helderheid: wie is in the lead? Ik denk dat die samenwerkingsafspraken ons in ieder geval gaan helpen om meer helderheid te geven aan de kritieke entiteiten, maar ik denk niet dat je 'm kunt aanwijzen in de wet zelf, juist vanwege de diversiteit van het landschap.

De heer **Van den Berg** (JA21):

Oké, dank. Als laatste nog over de zorgplicht. Ik hoor de minister zeggen dat ze één melding kunnen doen bij het punt en dat niet gelijk een boete zal worden opgelegd. Uiteindelijk zouden ze met één toezichthouder te maken hebben. Is de minister het desondanks met mij eens dat heel veel bedrijven de kaders, de criteria van de zorgplicht, toch onduidelijk vinden en daar zorgen over hebben? Zij begrijpen niet goed wanneer ze daar nu wel aan hebben voldaan en wanneer niet. Kan de minister daarop reflecteren? Hoe kan dat nu alsnog duidelijker gemaakt worden?

Minister **Van Weel**:

Dat is het werk dat nu moet gebeuren op basis van de Cyberbeveiligingswet zelf, en datgene wat er al aan handelingskader online staat bij de NCTV en het NCSC. Het self-assessment dat bedrijven kunnen doen, geeft veel inzicht in wat die zorgplicht zou behelzen. Uiteindelijk komen daar de ministeriële regelingen overheen, die per sector door de vakministers zullen worden uitgegeven. Die zullen nadere richtlijnen voor de specifieke sectoren bevatten, die ook houvast geven aan de bedrijven. Uiteindelijk zullen de toezichthouders in overleg met bedrijven uit de sectoren komen met nieuwe casussen die zij tegenkomen. Een aantal casussen zullen zij in die samenwerkingsafspraken al naar voren brengen. Dat netwerk bouwt zich langzaam op. We hebben er juist voor gekozen om dat niet vanaf het begin vanuit de ivoren toren in Den Haag te doen, maar dat over te laten aan de bedrijven en de sectoren, die meer kennis hebben over wat er specifiek nodig is in het kader van die zorgplicht.

Nogmaals, wat betreft de samenwerkingsafspraken kan ik 1 april nog steeds niet toezeggen, maar ik kan wel toezeggen dat deze zullen worden gepubliceerd in de Staatscourant om die helderheid te creëren. Dat gaat ook

over de betrouwbaarheid: wat u van toezichthouders kunt verwachten en wat een toezichthouder van u verwacht.

De **voorzitter**:

Dan heb ik nog een vraag over die loketfunctie. Ik ben heel blij met de toezegging dat dat loket er komt. Alleen sprak de minister toch nog over een ander loket voor twee andere richtlijnen. Onder het loket voor deze twee wetten worden ook nog andere dingen geschaard. Dat gaat dus om één loket. Maar daarnaast komt er toch nóg een loket. O, toch niet; ik zie de minister nee schudden. De vraag is: komen er nu twee loketten of gaat het zo veel mogelijk naar één loket?

Minister **Van Weel**:

Het gaat zo veel mogelijk naar één loket. Daarbij komen ook de twee andere richtlijnen die op andere sectoren van toepassing zijn samen. Eigenlijk krijg je een soort one-size-fits-all. De makkelijkheid voor bedrijven en entiteiten is dat ze één nummer bellen en naar één punt gaan. Dan is het aan ons om dat verder te geleiden.

De **voorzitter**:

Ik ben blij met deze beantwoording. Volgens mij kunnen we dan door naar het blokje toezicht.

Minister **Van Weel**:

Ja, daar zaten we al volop in. Ik zal even kijken welke vragen nog niet zijn beantwoord.

De samenwerkingsprotocollen komen eraan; dat is helder.

Ik heb ook uitgelegd waarom het niet mogelijk is om al op wetsniveau specifiek één toezichthouder aan te wijzen. Dat zou echt uit de samenwerking tussen de bestaande toezichthouders moeten blijken.

Een vraag van mevrouw El Boujdaini: hoe verhoudt de stelselverantwoordelijkheid van de minister zich tot het directeurenoverleg? Het directeurenoverleg is een van de onderdelen van het stelsel en is specifiek gericht op het toezicht. Het bestaat daarmee naast de andere onderdelen van het stelsel, zoals de samenwerking tussen CSIRT's onderling en de publiek-private informatie-uitwisseling. In het kader daarvan is er regelmatig contact over de afstemming tussen de toezichthouders en de

NCTV. Die rapporteren dan weer aan mij als minister. Zo zitten we samen in het speelveld.

Worden die samenwerkingsafspraken uiteindelijk in alle sectoren gemaakt? Ja, uiteindelijk dekken die alle sectoren af.

Worden organisaties ook nog geconsulteerd bij de afspraken die er worden gemaakt? In principe is het nu strikt een samenwerkingsafspraak tussen de toezichthouders zelf. Die kennen hun sectoren natuurlijk wel heel goed. In die zin denk ik dat de belangen van organisaties wel zullen worden meegenomen in diverse vraagstukken, maar zij zitten daar niet aan tafel om hun eigen toezicht in te regelen. Uiteindelijk horen de toezichthouders wel wat er speelt in een organisatie. Ik ga ervan uit dat zij dat ook meenemen.

Is het helder wie het eerste aanspreekpunt is bij toezicht, handhaving en incidentenafhandeling? Ja, er zit een doorverwijsboom bij de Cyberbeveiligingswet. Die staat op de website van de NCTV. Daarnaast gaan de samenwerkingsafspraken daar natuurlijk nog meer helderheid in creëren, met name voor bedrijven die tussen verschillende toezichthouders opereren.

Er werd gevraagd hoe ik aankijk tegen boetes en de methodes van andere landen. Ik denk dat die niet afwijken van de praktijk die we in Nederland zullen zien. Ook hier zul je niet in één keer de maximale boete krijgen. Dat is niet het enige sanctiemiddel. Ook hier zullen toezichthouders beginnen met waarschuwingen en pas bij herhaaldelijk overtreden overgaan tot sancties. Dat is normaal in onze rechtsgang in dit land.

Ik heb het gehad over dubbele beboetingen. Dat betreft overigens artikel 5:43 van de Algemene wet bestuursrecht.

Zien de structurele middelen in de memorie van toelichting ook op de extra capaciteit bij uitvoeringsdiensten zoals de ILT en de NVWA? Ja. De door de vakdepartementen geraamde structurele middelen geven een integraal financieel beeld. Dat is dus inclusief de toezichtslasten. Dat is indirect ook een antwoord op de vraag van mevrouw Kathmann of toezichthouders hiervoor worden uitgerust. De Cyberbeveiligingswet ziet op een significante uitbreiding van de taken en de scope van de doelgroep. Dat betekent dus ook dat die ziet op toezichtveranderingen met financiële gevolgen. De capaciteit voor het toezicht moet groeien vanwege de toename van het aantal entiteiten. Daarmee is rekening gehouden in deze wet.

Worden boetes dan ook proportioneel gezien ten opzichte van schaal, draagkracht en omzet van een entiteit? Omzet, schaal en draagkracht zijn relevante aspecten bij het bepalen van de hoogte van een boete. Toezichthouders zijn altijd gehouden aan de Algemene wet bestuursrecht en aan de algemene beginselen van behoorlijk bestuur. Een boete wordt dus altijd afgestemd op de ernst van de overtreding en de mate waarin die een entiteit te verwijten is. Dat geldt ook voor het proportionaliteitsbeginsel. Dat betekent dus dat de nadelige gevolgen van een boete voor een entiteit, een

bedrijf, niet onevenredig mogen zijn in verhouding tot de met het besluit te dienen doelen. Dat ondervangt dus in algemene zin het risico dat werd genoemd dat een bedrijf een boete als fooi beschouwt versus dat zo'n boete voor een bedrijf bijna desastreus zou zijn. Dat wordt ondervangen met dit proportionaliteitsbeginsel. Meestal hebben toezichthoudende instanties in hun boetebeleid ook een omschrijving van hoe ze de omvang van de organisatie meewegen in de hoogte van de boetes. Draagkracht telt daarin mee.

Toezicht op de kerncentrale. Wie houdt het toezicht op een incident bij een kerncentrale: de minister of de ANVS? Dat was een vraag van mevrouw Faber. De ANVS houdt toezicht op de kerncentrale voor de stralingsbescherming en de nucleaire veiligheid. Daarvoor is al uitgebreide sectorale wetgeving. De RDI is de instantie die toezicht houdt vanuit het perspectief van de leveringszekerheid van elektriciteit. Een kerncentrale kent dus alweer verschillende entiteiten. Uiteindelijk is de afweging om daar als Defensie ook nog bescherming aan te leveren. Die hangt dan weer vast aan de nationale dreiging die er wordt gezien jegens een bepaald object. Die wordt door sommige landen ook anders gewogen dan door andere.

De **voorzitter**:

Bent u klaar met het blokje?

Minister **Van Weel**:

Ik heb er nog twee.

De **voorzitter**:

Oké, nog twee. Dan kom ik daarna gelijk bij u, mevrouw Faber.

Minister **Van Weel**:

Hoe borgen we dat het toezicht en de ondersteuning niet achterblijven bij de enorme uitbreiding van de doelgroep? Dat is dus meegenomen in de samenwerkingsafspraken, de memorie van toelichting en de intensiveringsgelden die daarvoor zijn genoemd.

Dat was al de laatste vraag. De kosten van toezicht zijn daarmee dus gedekt, via de vakdepartementen.

De **voorzitter**:

Dat brengt ons meteen bij mevrouw Faber.

Mevrouw **Faber** (PVV):

Even over de kerncentrale. Er moest toen een zbo worden opgetuigd omdat men zelfstandig moest kunnen beslissen inzake de veiligheid, maar er zijn natuurlijk ook andere belangen. De minister gaf al aan dat een andere organisatie gaat over het leveren van elektriciteit, maar dan is natuurlijk wel de vraag wat dan voorgaat. Gaat de veiligheid voor of gaat voor dat men elektriciteit moet kunnen leveren? Ik denk namelijk dat dat op zich een essentiële vraag is. Het kan namelijk best zo zijn dat een kerncentrale onder druk staat en eigenlijk stilgelegd moet worden, maar dat het gevaarlijk kan zijn omdat men zegt: je moet leveren. Wat is dan de doorslaggevende factor in dezen?

Minister **Van Weel**:

Dat vind ik een interessante vraag. Daar heb ik oprecht het antwoord niet op. Ik weet ook niet of ik dat voor de tweede termijn heb. Ik wil dat in ieder geval meegeven aan een van de toezichthouders als een van de casussen. Ik kom daar dan op een later moment schriftelijk op terug.

Mevrouw **Faber** (PVV):

Ik had nog een andere vraag. Die ging ook over meerdere toezichthouders, ook als er bijvoorbeeld een zbo is. De minister heeft namelijk aangegeven dat er niet financieel ondersteund wordt. De minister heeft er niet voor gekozen dat kritieke entiteiten financieel ondersteund worden. Maar stel dat er twee vakministers zijn voor één entiteit en men dat uit de eigen begroting moet doen. Dan is er de kans dat ze de zaak naar elkaar toe schuiven om niet hun eigen begroting te belasten. En dan? Ik bedoel: is dat afgevangen?

Minister **Van Weel**:

Ja, ik vrees het wel. De afvanger zit hier voor u, want uiteindelijk ben ik de coördinerende minister voor het hele stelsel. Ik zal dan de beide vakministers bij elkaar moeten brengen en zorgen dat daar een oplossing voor komt.

Mevrouw **Faber** (PVV):

Dan de laatste vraag, voorzitter. Het is zo dat 80% van de entiteiten commerciële instellingen zijn. Daar heeft ook het Rijk toezicht op. Maar alles wat met de overheid te maken heeft, valt onder Binnenlandse Zaken. Daar is

de minister van Binnenlandse Zaken toezichthouder op. Maar dan controleert de overheid de overheid. Hoe gaat u dat dan scheiden, vraag ik via de voorzitter.

Minister **Van Weel**:

We kennen natuurlijk binnen de overheid meerdere toezichthouders, die weliswaar onder ministeriële verantwoordelijkheid vallen -- bijna allemaal in ieder geval -- maar zonder dat dit de onafhankelijkheid van hun bevindingen in de weg staat. De overheid kan de overheid controleren -- denk bijvoorbeeld aan de AP -- zonder dat dit compleet los hoeft te staan van de overheid.

Mevrouw **Faber** (PVV):

Ik denk dat de minister dit wel met de goede intenties vertelt, maar ik vind het toch een beetje vreemd. We hebben natuurlijk wel meer organisaties op afstand gezet van de overheid. Is dat dan bijvoorbeeld een zbo die dat doet? Welke constructie is er dan?

Minister **Van Weel**:

De RDI is een onafhankelijke instantie. De RDI valt weliswaar binnen de overheid, maar is wel een onafhankelijke instantie. Wat betreft de vraag of de RDI een zbo is, kijk ik of ik het antwoord daarop voor de tweede termijn voor u kan achterhalen. De RDI staat in ieder geval op afstand en heeft die onafhankelijkheid.

De heer **Van den Berg** (JA21):

Is het niet een beter idee om wettelijk te regelen dat het onafhankelijk toezicht op de overheidsinstanties op die manier wordt geborgd? Juist omdat we het hier hebben over kritieke entiteiten zijn juist de mensen die toezicht houden op deze entiteiten in principe kwetsbaar voor statelijke actoren, die deze mensen wel heel interessant zouden kunnen vinden. Zou het om de wet te versterken niet juist goed zijn om die aspecten wettelijk te borgen, zodat we nooit een samenloop hebben van belangen en toezicht?

Minister **Van Weel**:

We doen nu echt de overheid en de manier waarop wij ons toezicht hebben georganiseerd tekort. Ik heb zelf ook de Inspectie Justitie en Veiligheid. Ik heb geen enkele twijfel over de onafhankelijkheid van deze organisatie. Die geeft

mij ook gevraagd en ongevraagd adviezen, inspecteert en neemt die toezichthoudende taak uiterst serieus. Ik weet als bestuurder ook donders goed dat ik daar niet met mijn vingers tussen moet gaan zitten. We hebben talloze toezichtsorganen binnen de overheid, die weliswaar overheidsorganen zijn -- daar zou niemand anders voor willen betalen namelijk -- maar zonder dat we daarbij inhoudelijk tegen problemen aanlopen. Dat is bij de RDI, de toezichthouder in dit geval, dus ook het geval, maar ik kijk nog wel even naar wat precies de bestuursvorm is die daarvoor is gekozen, om die onafhankelijkheid te borgen. Dat heb ik aan mevrouw Faber toegezegd.

De heer **Van den Berg** (JA21):

Nou, hartstikke fijn. Ik weet niet of de minister dat zo bedoelde, maar ik wil wel onderstrepen dat ik niet een directe aanval wilde inzetten op de onafhankelijkheid van ambtenaren, want daar heb ik alle vertrouwen in. Mijn punt is natuurlijk meer dat als je dat kan scheiden en die belangen van elkaar kan ontvlechten … Het is natuurlijk wel een feit dat we juist bij deze entiteiten met zeer gevoelige informatie te maken hebben. Die risico-inschattingen gaan natuurlijk juist over onze kritieke processen. Juist daar moet je zeer vertrouwelijk mee omgaan. In die zin vind ik dat wel heel belangrijk. Maar dan nog over de toezichthouders. Ik heb begrepen dat er meerdere stelsels zijn waarin enerzijds het toezicht vanuit de overheid zelf wordt bekostigd. Andere zitten in een breder systeem, waarin bedrijven er gelden voor afstaan. Dat is in deze wet dan weer niet geregeld. Zou het in het kader van deze wet niet ook gewoon goed zijn als de overheid de bekostiging van de inspecties of de audits voor haar rekening neemt? Hoe kijkt de minister daarnaar?

Minister **Van Weel**:

Dat doen we al. In de memorie van toelichting is aangegeven wat de vakdepartementen denken nodig te hebben voor de implementatie van deze wetgeving. Daar zit de bekostiging van de individuele toezichthouders die zij hiermee belasten, al in. De reden waarom dat niet allemaal centraal is geregeld in deze wet, is omdat je nu eenmaal meerdere toezichthouders hebt. Die kun je niet afbakenen. We gebruiken de bestaande instituties en dat is dan ook weer in het kader van het verlagen van de regeldruk een van de proportionaliteitsmaatregelen van deze wet.

De heer **Van den Berg** (JA21):

Ik had van de audit een bedrag van volgens mij €432 in mijn hoofd, dat ik zag staan, maar daar kom ik dan nog even op terug. Als laatste nog de proportionaliteit van de boete. Het is heel fijn dat de minister erop reflecteert

dat we inderdaad altijd een bredere afweging maken, bijvoorbeeld de zwaarte van de overtreding en of het een herhaling is enzovoort. Maar het blijft naar mijn idee toch zo dat wanneer een bedrijf dat kleiner is -- laten we zeggen met een omzet van 100 miljoen euro -- een boete krijgt van in principe 10 miljoen euro, we te maken hebben met een zwaarte van 10%. Het blijft een feit dat wanneer een bedrijf groter is, 2% van de omzet wel het maximale boetebedrag blijft. Dat klopt volgens mij. Kunnen we er niet voor kiezen om dat te allen tijde proportioneel te houden, ondanks de zorgvuldige afweging van de toezichthouders?

Minister **Van Weel**:

Zoals ik al zei, hebben die dus vaak al boetebeleid, waar die proportionaliteit in staat en waarin dit soort aspecten worden meegewogen. Het feit dat een bedrijf over de kop zou gaan als het 2% van de jaaromzet moet afstaan, wordt dus meegewogen voordat de sanctie wordt opgelegd. Dat wordt dan ook weer afgewogen tegen wat iemand heeft gedaan en tegen de vraag of die daar wat aan kon doen. Die hele set van maatregelen is onderdeel van goed bestuur en dat zit al ingebakken bij die toezichthouders. Een maximumbedrag dat je meegeeft, is niet meer dan dat. Het is geen leidraad voor hoe zo'n toezichthouder uiteindelijk in de praktijk omgaat met die boetes, want die toezichthouder heeft gewoon te maken met de rechtsbeginselen van goed bestuur.

De heer **Van den Berg** (JA21):

Laatste vraag. Oké, fijn. Maar wat als we nu met een zeer groot bedrijf te maken hebben, bijvoorbeeld eentje met een jaaromzet van meerdere miljarden? Stel, je wilt zo'n bedrijf toch beboeten voor een overtreding die ze hebben begaan. Dan zitten we alsnog vast aan die maximale boete van 2% van de jaaromzet. In dat geval is de prikkel die we ze daarmee kunnen geven, dan weer relatief licht. Dat zie ik toch goed dan?

Minister **Van Weel**:

Nou, 2% van een heleboel of 2% van wat minder is in het eerste geval een heleboel. 2% van de jaaromzet van Apple zou ik graag terugzien op mijn begroting, laat ik het zo zeggen. Dat voelen die bedrijven ook.

De **voorzitter**:

U kunt verder met uw volgende blok en dat is volgens mij -- u weet dat beter dan ik -- actuele onderwerpen.

Minister **Van Weel**:

Ja, actueel en dat is vrij kort. Dat zijn maar twee onderwerpen, namelijk Odido en digitale soevereiniteit. Gaan deze wetten helpen om zaken zoals die bij Odido zijn gebeurd, te voorkomen? Dat kun je nooit garanderen, want we weten ook nog niet alle details van wat er bij Odido allemaal goed en fout is gegaan. Daar zal nog onderzoek naar gedaan worden. Maar de zorgplicht is er natuurlijk wel op gericht om dit soort incidenten te voorkomen. Daar zitten allerlei maatregelen achter, die de kans dat zoiets gebeurt, moeten verkleinen. Of het nu gaat over de omgang met data, de externe beveiliging, de training van personeel, cyberhygiëne, toegangsbeleid, beheer van assets: die hele waslijst valt onder de zorgplicht. Ik denk dat dat wel de drempel verhoogt, ook voor grotere organisaties, om dit soort zaken beter te kunnen voorkomen. En het toezicht gaat daarbij helpen, denk ik. Nogmaals, ik wil niet impliceren dat ik weet wat er bij Odido allemaal verkeerd is gegaan, maar ik denk dat deze wetten in algemene zin gaan helpen om dit soort incidenten te voorkomen in de toekomst.

Dan de digitale soevereiniteit. Kunnen we deze wet daar ook voor gebruiken? Ik wil het in mijn beantwoording houden bij de relatie tussen deze wetten direct. Ik wil de discussie over digitale soevereiniteit niet wegkapen bij mijn collega, de staatssecretaris van EZK. Maar deze beide wetten bieden wel de mogelijkheid om de risico's van de toeleverancierssketen aan te pakken. De vakminister kan entiteiten de verplichting opleggen om in bepaalde gevallen geen gebruik te maken van producten of diensten van specifieke leveranciers, wanneer dit noodzakelijk is voor de nationale veiligheid. We komen daar zo nog wat uitgebreider over te spreken. Dat is niet direct gericht op het vergroten van de digitale strategische autonomie, maar ik denk dat het wel een onderdeel is van een stap daarnaartoe. Entiteiten zullen die ook meewegen in hun inrichting en ook in hun strategische afhankelijkheden, die ze hebben laten gebeuren door hun afhankelijkheid van een bepaalde leverancier. De preventieve werking die dus mogelijk uitgaat van deze wetten, los van de specifieke ingrepen op nationale veiligheid, gaat in dat kader wel wat doen, denk ik. Verder zou ik de bredere discussie graag willen doorgeleiden naar mijn collega.

De **voorzitter**:

Dit was het blokje actuele onderwerpen. Ik kijk nog even naar links om te zien of er nog vragen zijn. We kunnen naar het volgende blokje: leveranciers.

Minister **Van Weel**:

Tot mijn spijt moet ik u wel zeggen dat mijn linkerblokje nog steeds hoger is dan het rechterblokje. Ik toets dat regelmatig aan u, maar wat dat betreft ben ik nog niet door de helft van mijn stapel papier.

De **voorzitter**:

Wij doen ons best aan deze kant van de Kamer.

Minister **Van Weel**:

Ik weet het. Ik geef u een update.

Waarom hebben we het weren van leveranciers in lagere regelgeving opgenomen in plaats van op wetsniveau? Dat hebben we gedaan omdat we het ook zien als de uitwerking van een zorgplicht. Dan is het niveau van een AMvB passend. Je wil ook niet alles in wetgeving vastleggen, omdat je ook wil kunnen inspelen op technologische ontwikkelingen. Er liggen ook nog twee amendementen voor met betrekking hiertoe en ik liet al even doorschemeren dat ik bereid ben om daar welwillend naar te kijken. Ik kom daar dus zo in de appreciatie nog op terug.

Overigens hebben we wel geluisterd naar het bedrijfsleven, dat natuurlijk naar aanleiding van de opname in de Cyberbeveiligingswet brieven naar ons heeft gestuurd. Die hebben we meegenomen in de nota van toelichting die bij de AMvB zit. We hebben daarin helder neergezet welke criteria gelden, om de voorspelbaarheid van het nemen van dit besluit en van de investeringen die ze moeten doen, groter te maken voor bedrijven. Daarbij wordt telkens getoetst aan dezelfde criteria en die staan nu dus in de nota van toelichting. Ook is daarin beschreven hoe de procedure voor de vakminister voorafgaand aan het nemen van het besluit dient te lopen. De betrokkenheid van de entiteit is ook meegenomen in die procedure. Bovendien kan de entiteit nog bezwaar en beroep instellen tegen het besluit.

Welke concrete criteria bepalen dat een leverancier een risico vormt? Er wordt gekeken of de leverancier de intentie heeft om schade aan te richten bij een entiteit of dat een entiteit nauwe banden heeft met of onder controle staat van een partij met kwade intenties. Dan kunt u denken aan leveranciers die via wetgeving verplicht kunnen worden om mee te werken met een buitenlandse overheid. Dat is dus een van de criteria, zoals ook door enkelen van u in vragen neergezet. Denk aan statelijke actoren met een offensief programma gericht tegen Nederlandse belangen. Al deze criteria staan in de toelichting van de AMvB.

Willen we daarbij ook kijken naar de mogelijkheid om financiële steun te geven bij het weren van een dienst of product? Dat was een vraag van mevrouw Kathmann. De Algemene wet bestuursrecht en daarbinnen de regels over nadeelcompensatie bepalen in elk geval op welke financiële

vergoeding men recht heeft als de overheid tussendoor de spelregels verandert, want daar komt het hier op neer, om goede redenen weliswaar. Dan is er automatisch sprake van recht op nadeelcompensatie. Dat zal elke keer door de vakminister worden bekeken. Ik kan daar dus niet in algemene zin uitspraken over doen. Ik zou willen voorkomen dat we op voorhand alle schade voor een leverancier vergoeden als we zo'n besluit zouden nemen, want daarmee halen we ook een stuk incentive weg bij entiteiten om zelf kritisch te kijken naar hun toeleverancierssketen, omdat de overheid, als het dan toch een keer aan het licht komt, daarvoor wel de portemonnee trekt. Dat zou ik ons collectief niet willen aandoen. Ik denk dus dat de nadeelcompensatie voldoet.

Dan ben ik bij overige belangrijke onderwerpen, voorzitter.

De **voorzitter**:

Ik kijk even naar links om te zien of mensen nog vragen hebben bij dit blokje. Dit was het blokje leveranciers. Nee, overig, toch? Nee, leveranciers; hierna komt overig.

De heer **Van den Berg** (JA21):

We hebben leveranciers gehad en nu gaan we naar overig.

Ik heb een vraag over de concrete criteria waarop we baseren dat een leverancier een risico voor de nationale veiligheid vormt. Ik hoorde de minister zeggen dat het bijvoorbeeld statelijke actoren zijn die een offensief cyberprogramma hebben richting ons. Op basis van welke feiten en omstandigheden stellen we deze landen vast? Ik kan me namelijk ook voorstellen dat daar een AIVD- dan wel een MIVD-component aan zit. Kortom, hoe kunnen we dit als parlement controleren?

Minister **Van Weel**:

Daar zit zeker een AIVD- en MIVD-component aan, en ook een NCTV-component. Maar er zit ook een openbare component aan. We proberen juist met dit soort zaken ook op structurele basis -- dit gaat over individuele gevallen, maar ik heb het dus over de structurele basis -- zo veel mogelijk van het dreigingsbeeld zoals wij en de diensten dat zien met uw Kamer te delen. Een voorbeeld daarvan is het Dreigingsbeeld Statelijke Actoren. In het laatste dreigingsbeeld wordt ook ingegaan op de vraag welke landen offensieve cyberprogramma's hebben tegen ons en welke risico's en concrete gevallen we daarvan zien. Dat is allemaal op ongerubriceerd niveau, maar geeft, denk ik, wel een aardig aanknopingspunt, ook voor entiteiten om te lezen waar ze beter niet mee in zee kunnen gaan of waar ze op enig moment

het risico lopen om tegen een knelpunt in de keten aan te lopen. Daarmee proberen we dus wel te helpen bij de afwegingen die entiteiten daarbij maken.

De heer **Van den Berg** (JA21):

Dat kan ik alleen maar ondersteunen. Dank u wel.

De **voorzitter**:

Minister, we kunnen naar het volgende blokje.

Minister **Van Weel**:

Het blokje overig. Ik begin bij de positie van slachtoffers. Is de positie van slachtoffers goed genoeg vastgelegd in deze wetten? Voor significante incidenten regelt de Cyberbeveiligingswet dat de betrokken entiteiten ontvangers van een dienst in kennis moeten stellen indien dat incident een nadelige invloed kan hebben op de verlening van die dienst. Ook wordt hierin geregeld dat de entiteit ontvangers van een dienst die door een significante dreiging in relatie tot die dienst kunnen worden getroffen, mee moet nemen in de vraag welke maatregelen zij daarvoor kunnen treffen. Er is echter geen specifieke regeling over de positie van slachtoffers opgenomen. Ik wil wel verwijzen naar een aangenomen motie van het lid Rajkowski waarin gevraagd wordt om te kijken naar de positie van slachtoffers en nadeelcompensatie. Ik zie een aantal van uw leden nu knikken. Dat proces loopt natuurlijk nog, maar staat los van deze Cyberbeveiligingswet. Dat gaat nadrukkelijk om slachtoffers.

Kunnen we kennisdeling over dreiging en kwetsbaarheden en aanvalspatronen beter organiseren, niet alleen in Nederland maar ook met landen om ons heen? Ja. Het doel met deze wet is juist om het delen van kwetsbaarheden en dreigingen, waaronder ook AI-gegenereerde cyberdreigingen, beter te organiseren en beter te verbreden. Het CSIRT krijgt hiervoor een specifieke grondslag in deze wet. Nationaal werken de CSIRT's al met elkaar samen in het CSIRT-netwerk. Ook internationaal is er een CSIRT-netwerk waarin dagelijks op operationeel niveau informatie wordt uitgewisseld. Nederland is ook actief in het CyCLONe-netwerk voor samenwerking bij crisissen en incidenten, en in de NIS Cooperation Group, waarin experts van Europese lidstaten leren van elkaars ervaringen en best practices. Daarnaast biedt de Cyberbeveiligingswet een nadrukkelijke grondslag om makkelijk informatie met derde landen zoals het Verenigd Koninkrijk te delen, ook informatie over aanvalspatronen.

Tot slot moeten we opmerken dat we naast de AI-gegenereerde dreigingen ook steeds meer AI-gegenereerde verdediging zien. Uiteindelijk gaat ons dat ook helpen. Ik kan me nog levendige discussies herinneren met de topmannen van Apple en Google over de vraag of de verdediging nou meer baat heeft bij AI of de aanval. Ik zal het u niet verklappen, maar de twee waren in ieder geval tegenovergesteld in hun opvattingen hierover. Ik denk dat de nabije toekomst het ons gaat leren.

Dan de informatie-uitwisseling in crisis, kritieke entiteiten en private beveiligingsbedrijven. Kunnen we daarbij versnippering en inefficiëntie voorkomen, was een vraag van mevrouw El Boujdaini. In eerste instantie moeten kritieke entiteiten zelf de verantwoordelijkheid nemen voor een crisisrespons en de daarbij behorende informatie-uitwisseling. Ze kunnen daar zeker private beveiligingsbedrijven in meenemen. De meeste doen dat overigens ook als zij een incident van een bepaalde omvang hebben. Elk ministerie neemt daarnaast maatregelen op het eigen beleidsterrein om crisissen aan te pakken. Daarvoor hebben ze allemaal een departementaal crisiscoördinatiecentrum. Bij een nationale crisis -- het is niet helemaal in beton te gieten wanneer dat gaat spelen, maar op enig moment schalen we op -- is er een nationaal crisiscentrum. Dat valt dan coördinerend onder mijn verantwoordelijkheid. Dat is een 24/7-informatieloket en ondersteunt ook de nationale crisisstructuur en alle partijen. Daarnaast zijn er sectorale afspraken gemaakt over informatie-uitwisseling. Een voorbeeld hiervan is het NCSC, dat binnen het cyberdomein zorgt voor gerichte informatiedeling tussen publieke en private partijen. Daarmee wordt versnippering voorkomen en efficiënte informatievoorziening tijdens crises gewaarborgd.

Mevrouw El Boujdaini vroeg ook hoe deze private beveiligingsbedrijven meer duidelijkheid kunnen krijgen over hun rollen. Ze hebben geen formele rol in deze wetten. Het is echt de verantwoordelijkheid van de kritieke entiteit om passende maatregelen te nemen, maar natuurlijk zullen zij gebruikmaken van private partijen -- daar is ook geen verbod op -- om te helpen bij de implementatie en naleving van deze wet.

De heer Vermeer vroeg of er duidelijkheid komt over wat wel of niet redelijk is om van leveranciers te eisen. Ja. Onder deze Cyberbeveiligingswet moeten entiteiten uitsluitend inzicht krijgen in leveranciers die van invloed kunnen zijn op de beveiliging van haar netwerk of informatiesysteem. Dat is meteen een afkadering voor hoe diep je in die food chain, zeg ik hier maar even letterlijk, moet gaan om te kijken waar het relevant is en waar niet. De entiteiten toetsen of er door de leveranciers wordt voldaan aan de beveiligingseisen. Dat kan met een certificering van de toeleveranciers of clausules in de leveringsovereenkomsten die zij sluiten.

Hoe voorkomen we dat grote ketenpartners hun verantwoordelijkheden afwenden op kleine ondernemers? Die verantwoordelijkheid kán niet worden afgewenteld door grote entiteiten; die staan per definitie aan de lat in het kader van deze beveiligingswet. Zij moeten zelf inzicht krijgen en uiteindelijk

toetsen kunnen doen voor hun toeleveranciers, maar er ligt dus ook een gedeelde verantwoordelijkheid om die te certificeren.

Voorzitter. Als het gaat om de bewaartermijnen, ben ik even in handen van uw Kamer. Ik heb gezegd waarom er een onderscheid is tussen de CSIRT's en de toezichthouders, maar ik weet niet of dat voldoende helder was. Ik kan er alleen aan toevoegen dat elke toezichthouder wel per dossier kijkt of de termijn van 60 maanden noodzakelijk is. Daar hebben ze al processen voor. In die zin sluiten deze wetten aan bij wat al gebruikelijk is voor toezichthouders in een toezichthoudende rol in den brede.

De motie van mevrouw Rajkowski over het handelingskader voor slachtoffers van datalekken had ik al genoemd. Die was van 10 maart. Daar wordt aan gewerkt.

Dat was het einde van mijn blokje.

De **voorzitter**:

Dit was het blokje overig. De heer Van den Berg heeft een vraag, en dan heeft mevrouw Zwinkels een vraag.

De heer **Van den Berg** (JA21):

Nog even over het opslaan van de gegevens. Als ik het goed lees, zou het gaan om maximaal 120 maanden voor de toezichthouders. Voor overige wettelijke taken geldt een maximale bewaartermijn van 60 maanden. Hoe kijkt de minister dan naar die tien jaar? Is dat niet veel te lang? Zou dat niet korter kunnen? Kan de minister bevestigen dat die tijd niet elke keer opnieuw gaat lopen? Volgens mij is het zo aangepast dat de juistheid van de gegevens bevestigd moet worden. Ik vraag mij af wat nu het ijkpunt is dat bepaalt wanneer de opslag van die gegevens verlengd wordt.

Minister **Van Weel**:

Die termijn van 120 maanden is echt gericht op die gevallen waarin er specifieke juridische procedures lopen. Die kunnen echt rustig vijf jaar in beslag nemen. Ik ken deze zaken ook nu binnen het ministerie. Er zijn gewoon zaken die zo'n lange looptijd hebben. Als je dan aanloopt tegen de wettelijke bewaartermijn van je gegevens, dan komt zo'n zaak in gevaar, terwijl je een zaak ook niet sneller kunt laten gaan dan die gaat. Het betreft dus wel echt een maximumtermijn. Het is niet zo dat het streven is om al die gegevens tien jaar te bewaren. Als je al die trajecten doorloopt van een zaak, en dan het beroep en het hoger beroep, kun je uiteindelijk wel tegen die termijnen aan lopen, maar dat is zeker niet de norm.

De heer **Van den Berg** (JA21):

Helder. Maar hoe werkt het dan in de praktijk? Hoe wordt per dossier beoordeeld of een kortere bewaartermijn toch mogelijk is? Hoe wordt ervoor gezorgd dat het in de praktijk niet alsnog zo uitpakt dat we die gegevens gewoon laten staan?

Minister **Van Weel**:

Daar hebben toezichthouders hun eigen procedures voor. Die zijn er overigens niet naar aanleiding van deze wetten, maar dat geldt voor alles wat ze aan toezichthoudend werk doen. De criteria op basis waarvan ze hun bestanden vegen, zijn dus een-op-een van toepassing hierop. Daarom sluiten we ook aan bij de termijnen zoals ze die kennen, ook voor hun reguliere toezichtwerk.

Mevrouw **Zwinkels** (CDA):

Ik ben blij met het antwoord rondom de cyberaanvallen die tot stand komen met AI. Ik ben ook benieuwd of we daarover kunnen worden geïnformeerd als het gaat om de samenwerking met andere Europese lidstaten te zijner tijd. Mijn vraag is eigenlijk tweeledig. Ik heb nog twee gemiste vragen, want dit was het blokje overig en volgens mij het laatste blokje.

De **voorzitter**:

Nee, niet het laatste blokje. Hierna komen we pas bij de wet.

Mevrouw **Zwinkels** (CDA):

O, oké. Dan kan ik het heel kort aankondigen. Dan weet ik of de minister er nog op ingaat. Ik had nog een vraag over de gekwalificeerde vertrouwensdiensten en over de uitvoeringscapaciteit bij ILT en NVWA. Als die aan bod komen, zijn mijn vragen verder allemaal beantwoord vandaag.

Minister **Van Weel**:

Dat houden we in ieder geval in gedachten. Die tweede vraag heb ik beantwoord. Die gaat over dat in de memorie van toelichting is meegenomen dat vakdepartement datgene wat nodig is aan capaciteit bij de verschillende toezichthouders, waaronder de twee die u noemt ... Die zitten ook in deze

wet. De eerste vraag hoop ik nog tegen te komen, want it doesn't ring a bell now.

De **voorzitter**:

Anders kijken we zo naar die twee blokjes.

Minister **Van Weel**:

Voorzitter, ik denk dat ik een heleboel uit die wetsblokken al gehad heb, maar ik zal er met prudentie doorheen gaan.

De **voorzitter**:

Ik heb nog twee vragen voor u. De eerste gaat over de slachtoffers. Ik had het over letterlijk een nazorgplicht opnemen in de wet. U wijst terecht naar de motie over het handelingskader van mevrouw Rajkowski, want dat is niet voor niks een heel breed ondersteunde motie. Zij vroeg of er in ieder geval een groter handelingskader zou komen, zodat we in ieder geval iets kunnen, want we hebben gewoon gezien, zowel na het lek bij het bevolkingsonderzoek baarmoederhalskanker als nu bij Odido, dat mensen echt in paniek zijn. Bij het baarmoederhalskankeronderzoek zijn nog steeds heel veel vraagtekens. Mensen weten veel gewoon niet. Waar moeten ze heen als ze willen weten wat er is gelekt? Waar moeten ze heen als ze iets willen vervangen? Hoe regelen ze dat? Waar krijgen ze hulp? Het handelingskader van mevrouw Rajkowski is dus fantastisch, alleen is de vraag: zouden we niet toch nog echt expliciet iets in de wet willen opnemen hierover?

Minister **Van Weel**:

Ik heb een aantal specifieke punten genoemd die wel zien op zorg naar afnemers van diensten, op entiteiten en op de verplichting die bedrijven op basis van de Cyberbeveiligingswet hebben om daar wat mee te doen. Ik sta niet onsympathiek tegenover uw gedachten over nazorg, maar ik zou het heel graag willen koppelen aan de verkenning die we doen naar aanleiding van de motie-Rajkowski en dat daar ook in meenemen, zodat we ook een gedegen grond hebben op basis waarvan we dan beleid gaan maken. Ik voel uw gedachten dus zeker.

De **voorzitter**:

Dank voor deze beantwoording. Ik heb toch nog een vraag. Ik vond namelijk dat de minister best kort door de bocht ging over de bewaartermijnen. Het is heel fijn dat er echt goed wordt nagedacht. Soms kan je gewoon minder lang opslaan dan wettelijk noodzakelijk. Maar we weten nu al hoe vaak het misgaat met: wettelijk noodzakelijk is het niet, maar we doen het lekker toch. Hoe gaan we er echt goed op toezien dat gewist wordt wat gewist kan worden? Hoe gaan we dat explicieter maken, zodat we daar als Kamer gewoon beter zicht op hebben en dat echt gaat gebeuren? Daar gaan namelijk juist de grote risico's van uit.

Minister **Van Weel**:

Dat ben ik met u eens. Ik denk alleen niet dat deze groep daarin de grootste risicogroep is. Over het algemeen zijn toezichthouders redelijk prudent met betrekking tot de omgang met gegevens. Ik denk dat dit in bredere zin een issue is. Dat heeft het Odidolek ook wel op de kaart gezet. In hoeverre wordt er toegezien op het wissen van gegevens op het moment dat het niet langer noodzakelijk is om die te bewaren? Dat geldt voor overheidsinstanties en evengoed voor bedrijven en hun omgang met persoonsgegevens. Ik vind dat dus een bredere vraag. Ik vind ook dat we die moeten oppakken, maar niet binnen de scope van deze wet, want die termijnen zien echt op de toezichthouders en daar heb ik eigenlijk de minste zorgen over.

De **voorzitter**:

Dan gaan we naar het een-na-laatste blokje, de Cbw.

Minister **Van Weel**:

Nou, ik begin nog even met Caribisch Nederland en de toepassing. Sorry, voorzitter, die heb ik er nog even tussen gefietst. Daarmee wil ik zeker niet zeggen dat we dit niet van belang vinden, want natuurlijk willen we Caribisch Nederland op hetzelfde niveau krijgen als de rest van Nederland. Maar we hebben wel te maken met de lokale uitvoeringscapaciteit. Dat beïnvloedt het tijdpad dat we daar kunnen lopen. We moeten dus gaan voor een verantwoorde stapsgewijze invoering. We gaan eerst bekijken welke ondersteuning we daarbij kunnen bieden zonder dat we afbreuk doen aan de lokale verantwoordelijkheid die er daarvoor ligt. Ik heb trouwens wel de ambitie om voor het Caribisch deel van het Koninkrijk te komen tot een cybersecuritystelsel op hetzelfde niveau. Dat zit ook in de Veiligheidsstrategie van het Koninkrijk der Nederlanden. Daarom zit Caribisch Nederland ook specifiek in het Cyberweerbaarheidsnetwerk. We hebben een eerste verkenning gedaan naar de uitrol van het bouwplan. Daaruit blijkt dat er behoefte is aan verankering van de digitale weerbaarheid en het

cybersecuritystelsel in Caribisch Nederland. Vanwege de digitale afhankelijkheden erkennen we de noodzaak om hierin gezamenlijk op te treden met Aruba, Curaçao en Sint-Maarten, maar daarbij moeten we natuurlijk ook wel letten op de autonome status van deze landen, want zij bepalen hun eigen landniveaus met betrekking tot cybersecurity. Zij moeten dus ook het belang zien van het samenwerken hierin, maar daar spannen we ons wel voor in.

Ik heb hier nog wat varianten op hetzelfde. Ik kan er nog een ding aan toevoegen, namelijk dat het mogelijk is om de toepassing van de wet mee te nemen richting de eerste evaluatietermijn. Die toezegging kan ik de heer Van den Berg wel doen, maar ik heb wel gezegd dat de randvoorwaarden ter plekke gaan bepalen hoe snel we hierin kunnen gaan. Dat gaan we in gezamenlijkheid doen. Dat was het blokje Cariben.

De **voorzitter**:

Dit was wel het einde van het blokje. Ik kijk even naar links om te zien of de Kamerleden vragen hebben. Er is een vraag van mevrouw El Boujdaini.

Mevrouw **El Boujdaini** (D66):

Dank voor de beantwoording, zeg ik via de voorzitter. Ik ben blij te horen dat in ieder geval wel wordt gezien dat het belangrijk is dat ook daar het beschermings- en weerbaarheidsniveau echt op orde zijn. Ik heb met mensen van daar gesproken. Er is daar wel echt heel veel behoefte aan meer inzicht in wanneer we daar dan kan kunnen komen en wat daar precies voor nodig is. We hebben inderdaad de Veiligheidsstrategie van het Koninkrijk. Dat is een goede basis, maar die is nog niet echt toereikend genoeg. Daarom wil ik de minister toch vragen of er een routekaart zou kunnen komen om wat meer perspectief te kunnen bieden op hoe we nou echt tot dat beschermings- en weerbaarheidsniveau kunnen komen en wanneer we dat voor elkaar kunnen krijgen, samen met hen natuurlijk.

Minister **Van Weel**:

Ik ga die vraag doorgeleiden naar mijn collega, de staatssecretaris van BZK, omdat die naar de integraliteit van het Koninkrijkspakket kijkt. Ik vraag hem dit mee te nemen.

De **voorzitter**:

Dan gaan we naar het een-na-laatste blok.

Minister **Van Weel**:

Ik ga er zo snel als ik kan doorheen, voorzitter: de Cbw. Waarom heeft de implementatie zo lang geduurd? Ik denk dat ik dat aan het begin van mijn inleiding eigenlijk al gezegd heb. Wij hebben ervoor gekozen om ervoor te zorgen dat alles werkt voordat we verklaren dat de wet van toepassing is, in plaats van de wet van toepassing verklaren en dan maar kijken hoe we het gaan invullen. Dat kost tijd, maar komt de zorgvuldigheid ten goede, en uiteindelijk ook de werkbaarheid, denk ik. Wat dat betreft ben ik blij dat we er zijn.

Over evalueren hebben we het gehad.

Mevrouw Kathmann vroeg welke CSIRT's worden aangewezen voor de sectoren en welke nieuwe er nog worden opgericht. Voor de meeste entiteiten wordt de minister van Justitie als CSIRT aangewezen. De bijbehorende taken worden namens mij uitgevoerd door het NCSC. De andere Cyber Security Incident Response Teams zijn Z-CERT voor de zorgsector, CERT Watermanagement -- de naam zegt het eigenlijk al een beetje, maar dan in het Engels -- de Informatiebeveiligingsdienst voor gemeenten en SURFcert voor de onderwijssector. Op dit moment hebben we geen zicht op nieuwe CSIRT's die worden opgericht.

Hoe kunnen de gegevens van die CSIRT's nou goed beveiligd worden? Welke technische veiligheidsmaatregelen zijn er daarvoor? De NIS2-richtlijn stelt hele strenge eisen aan CSIRT's. Een van die eisen is dat de ondersteunende informatiesystemen zich op beveiligde locaties bevinden. Een andere eis is de betrouwbaarheid en de vertrouwelijkheid van de activiteiten van het CSIRT. Die zijn bij ons vastgelegd in het Cyberbeveiligingsbesluit, dus in de AMvB. In aanvulling daarop kunnen bij ministeriële regeling nadere functionele, technische en organisatorische eisen worden geregeld. Verder ga ik in het openbaar niet heel veel uitspraken doen over de techniek, om evidente redenen.

Dan de vraag van mevrouw El Boujdaini over tijdige informatiedeling met de burgemeesters en de voorzitters van de veiligheidsregio's. Laat ik beginnen door te zeggen dat ik ook voorzitter ben van het Veiligheidsberaad en van het Landelijk Overleg Veiligheid en Politie. Ik ben dus zeer begaan met onze nationale veiligheid, de structuren die we daarvoor hebben en de individuele verantwoordelijkheden. Maar ik worstel een beetje met de manier waarop de informatiedeling op basis van deze wet zou moeten verlopen, omdat het voor de CSIRT's die bezig zijn met de calamiteit at hand onmogelijk is om te overzien welke fysieke gevolgen voor de openbare orde en veiligheid dat dan waar zou hebben. Denk aan wat er is gebeurd met Odido. Odido heeft een hoofdkantoor, waarschijnlijk ergens op de Zuidas in Amsterdam. Is het dan relevant voor de burgemeester van Amsterdam om te worden ingelicht over een datalek bij Odido? Ik denk het niet direct. Ik denk dat dit een landelijk

kader vereist. Dat hebben we ook gezien; dat groeit dan automatisch. Maar als je bijvoorbeeld een hack hebt bij een waterschap, dat impact heeft op een bepaalde polder en gemeenschap, dan wil je natuurlijk dat de informatie wel daar terechtkomt. Maar dan loopt de lijn eigenlijk vaker via de kritieke entiteiten dan via CSIRT en de Cyberbeveiligingswet. Ik ben dus huiverig om die triagetaak, om het zo maar te zeggen, neer te leggen bij de mensen die bezig zijn met het cyberincident, omdat ze dan ook nog moeten afwegen of er een link is met de fysieke openbare orde of niet en wat ze dan moeten doen. Eigenlijk heb ik tot nu toe altijd gezien dat als de gevolgen groter worden -- denk aan geen treinverkeer -- de route van de fysieke openbare orde en veiligheid zich wel redt, maar dan buiten deze wet om.

Dan de vraag van mevrouw Kathmann over Amerikaanse ICT-diensten. Ik heb het gehad over de criteria die gelden, maar ik wil hier nu niet ingaan op specifieke landen, casussen of wat dan ook. Ik denk dat de criteria voldoende aanknopingspunten bieden, ook voor entiteiten, om na te kunnen denken. Ik wil me nu alleen even niet wagen aan landen.

Mogen de OKTT-organisaties nog steeds relevante dreigingsinformatie ontvangen om te delen met hun achterban? Het antwoord is ja. Zij zijn in de Cyberbeveiligingswet een andere relevante partij en daarmee hebben ze die bevoegdheid nog steeds.

Gekwalificeerde vertrouwensdiensten -- daar is ie! Namens de staatssecretaris Digitale Economie en Soevereiniteit kan ik vertellen dat geprobeerd wordt om het gebruik van gekwalificeerde vertrouwensdiensten op te nemen in de "pas toe of leg uit"-lijst. Dit is een set van verplichte open standaarden voor ICT-inkoop door de overheid. De "pas toe of leg uit"-verplichting over het gebruik van open standaarden geldt voor gemeenten, provincies, het Rijk, waterschappen en alle uitvoeringsorganisaties. Dat betekent dat de standaarden die op de lijst staan in principe moeten worden gebruikt, tenzij er serieuze redenen zijn dat ze niet kunnen worden gebruikt. Dat heeft tevens een krachtig effect op en uitstraling naar de private sector. Het is echter niet zeker of opname op de lijst gaat lukken. Daarom zal samen met de staatssecretaris worden onderzocht welke alternatieven daarvoor zijn. Zij verwacht uw Kamer hierover voor het einde van het jaar te kunnen informeren. Ik zie dat er een vraag is, maar ik hoor de voorzitter aangeven dat die aan het einde van het blokje moet. Ik leg het mapje voor de zekerheid even apart!

Het basispakket cyberveiligheid, zoals geopperd door mevrouw Kathmann. Ook ik vind dat cyberveiligheid ook voor individuele burgers, ongeacht de draagkracht, van belang is. Je kunt immers tegenwoordig niet meer om het digitale leven heen, wat verder ook je leefomstandigheden zijn. Tijdens het wetgevingsoverleg BZK heeft u hierover gesproken met mijn collega's. Mijn collega van EZK heeft hierover opgemerkt: "Diverse marktpartijen bieden veiligheidspakketten aan. Een deel van de genoemde producten wordt gratis aangeboden." Zij heeft aangegeven dat ze met de aanbieders van deze

producten de inhoud en de toegankelijkheid van het aanbod wil bezien en dat ze wil kijken hoe die eventueel verbeterd kunnen worden. Wat haar betreft moet de overheid niet concurreren met de markt. Dat mag volgens de Wet markt en overheid namelijk ook niet. Het is wel belangrijk dat dergelijke pakketten door de markt worden aangeboden. U heeft tijdens dat debat inderdaad een motie aangehouden, mevrouw Kathmann.

Mevrouw Kathmann vroeg ook wat ik ga doen om de rollen van de vakministers, de toezichthouders en de sector zo goed mogelijk vast te leggen. Ik noemde de doorverwijsboom al. Die geeft helderheid over waar je in het landschap hoort. Hij geeft in ieder geval een overzicht van welke partijen erbij betrokken zijn. Onderling hebben we het al gehad over de samenwerkingsprotocollen en afspraken van bijvoorbeeld de toezichthouders. Die moeten meer helderheid geven voor individuen.

Dat is volgens mij de Cyberbeveiligingswet, voorzitter.

De **voorzitter**:

Dan zijn we aan het einde van het blokje. Mevrouw Zwinkels had sowieso een vraag. Daarna komt mevrouw El Boujdaini.

Mevrouw **Zwinkels** (CDA):

Mijn vraag gaat over de gekwalificeerde vertrouwensdiensten. Ik begrijp van de minister dat hij ook namens de staatssecretaris beantwoordt. Ik kan me dus voorstellen dat het lastig is om er inhoudelijk verder op in te gaan. Ik ben blij met de toezegging om er voor het einde van het jaar op terug te komen, maar ik zou natuurlijk ook graag willen weten waarom het eventueel niet lukt om het op de lijst te krijgen waar de minister het over had. Dan zou ik daar vanuit de Kamer namelijk wellicht op kunnen bijsturen. Nogmaals, ik snap dat de inhoudelijke beantwoording voor nu misschien tot hier reikt, maar ik zou het kabinet via de minister willen meegeven dat ik daar tijdig over wil worden geïnformeerd. Zo kunnen we daar voor het einde van het jaar eventueel nog iets aan doen.

Minister **Van Weel**:

Deze boodschap neem ik graag mee naar mijn collega van EZK.

Mevrouw **El Boujdaini** (D66):

Ik wil graag terugkomen op de beantwoording van de minister van mijn vraag over de informatiepositie van burgemeesters en de veiligheidsregio's. We zijn

eigenlijk op zoek naar een wettelijke grondslag om op te kunnen voortbouwen. De burgemeesters en de veiligheidsregio's zijn verantwoordelijk voor crisisbeheersing en ordehandhaving. We willen juist hen meer in hun kracht zetten. Ik heb ook voorbeelden uit de praktijk. Afgelopen jaar was er hier in Den Haag een stroomstoring. Daardoor viel bijvoorbeeld het ov stil en ontstond er verkeerschaos. De gemeente zelf was in de veronderstelling dat het ging om een cyberincident, een cyberaanval, terwijl landelijk het NCC al een analyse had gemaakt en had geconcludeerd dat het niet om een cyberaanval ging. Lokaal waren ze daar nog niet van op de hoogte. Lokaal kan het de gemeentes dus juist enorm versterken als ze dit soort informatie krijgen. Zo kunnen ze werken aan preventie voor in de toekomst, maar ook sneller ingrijpen en sneller beslissen wat er nodig is om de orde te handhaven en de crisis te beheersen. Ziet de minister het ook zo, als ik het op deze manier en met dit voorbeeld uitleg?

Minister **Van Weel**:

Ik vind het op zich een aansprekend voorbeeld, maar het hoort voor mij thuis in de categorie dat dingen op een gegeven moment impact gaan en kunnen hebben op de openbare orde en veiligheid. Ik zie dan al heel snel een taak voor mijzelf dan wel voor mijn vakcollega's naar boven komen. Op het moment dat er een grote verstoring is in het ov, staat de staatssecretaris van IenW daarvoor aan de lat en pakt die dat samen met het lokale en regionale bestuur op, zoals ik dat doe als het gaat om -- ik noem maar wat -- de dreiging richting de Joodse gemeenschappen in heel Nederland. Als er dan fysiek iets moet gebeuren, is dat uiteindelijk aan de burgemeesters en de veiligheidsdiensten. Ik zie mezelf dan als de hoeder van die informatie.

Ik vind het lastig om wettelijk vast te leggen dat er een brengplicht is van specialistische organisaties naar specifieke burgemeesters, waarvan erg moeilijk op voorhand is in te schatten of er überhaupt een relatie met de openbare orde en veiligheid is of niet. En als die er wel is, is die dan heel lokaal af te bakenen? Waar moet die dan neerslaan? Dat vind ik buiten de scope. Ik zou daar dan weer mensen van mijn crisiscentrum op moeten zetten die continu met die bril kunnen kijken naar alles wat er afgehandeld wordt, terwijl ik het eigenlijk andersom zie: op een gegeven moment bereikt iets een bepaalde schaal, waarna deze raderen in beweging komen. Ik zit dus even te denken of we u nog kunnen helpen middels een motie die de geste hiervan draagt, namelijk dat er zorg gedragen moet worden voor, indien relevant, informatie richting burgemeesters als een significant cyberincident een lokaal gevolg zou kunnen hebben voor de openbare orde. We kunnen dan iets vrijer laten wie dat moet doen en op welk moment, zodat het ook niet heel diep in die wet zit. Dan zou ik er wel voor openstaan om daarover mee te denken.

Mevrouw **El Boujdaini** (D66):

Fijn dat de minister ervoor openstaat om mee te denken. De andere kant hiervan is namelijk wel dat als we dit niet goed regelen, het weer aan de gemeenten zelf is om afspraken te maken met de verschillende kritieke entiteiten. Het is best een grote uitvoeringslast voor de gemeenten om per kritieke entiteit te kijken hoe je informatie uitwisselt. Eigenlijk is er al een centraal informatiepunt, want het NCSC heeft een monitoringsverantwoordelijkheid. Dat heeft de informatie sowieso al en hoeft die in principe alleen door te geleiden. Ik denk dat ze lokaal inderdaad ook best wel goed kunnen inschatten wanneer ze welke informatie kunnen gebruiken. Zoals ik eerder al aangaf in mijn betoog, heb ik hier ook een amendement op ingediend. Ik denk dat we later nog op de appreciatie daarvan komen. Laten we die afwachten. Anders sta ik er zeker voor open om te kijken wat we wat dat betreft middels een motie kunnen doen, maar het liefst heb ik natuurlijk het amendement.

De **voorzitter**:

Dank. Minister, wilt u nog ...

Minister **Van Weel**:

Ik had al zo'n vermoeden. Kijk, informatie is waardeloos zonder duiding. Als minister van nationale crises ben ik het meest beducht voor mensen die zomaar informatie neerleggen op plekken zonder dat daar een handelingsperspectief of wat dan ook bij komt. Het NCSC is naar mijn mening niet in staat om de informatie met die duiding en het handelingsperspectief op de goede manier neer te leggen bij de burgemeester. Ik zie wel een taak voor mezelf op het moment dat iets groter wordt, of voor de NCTV vanuit de crisisstructuur die we hebben. Dus ik zie het probleem. Alleen, ik voorzie een andere weg naar de oplossing. Ik neem u echt heel serieus wat dat betreft, maar ik wil voorkomen dat mijn lieve mensen van het NCSC een rol gaan spelen in de lokale crisisbeheersing in plaats van gewoon de digitale problemen op te lossen.

De **voorzitter**:

Mevrouw El Boujdaini, ik zie dat u nog een vraag heeft.

Mevrouw **El Boujdaini** (D66):

Nog één laatste, ja. Misschien is het niet helemaal een vraag. Het is inderdaad niet de bedoeling van mijn fractie om heel veel uitvoeringslast

neer te leggen bij het NCSC. Juist omdat het NCSC sowieso al het centrale punt is voor informatieverzameling, is het relatief ten opzichte van de gemeentes die anders zelf een-op-een afspraken moeten maken met de kritieke entiteiten om bepaalde informatie binnen te halen. We hebben geprobeerd om daarin een balans te vinden. Ik zou het heel fijn vinden als we een weg kunnen vinden om dit voor iedereen werkbaar te maken en de lokale bestuurders in hun kracht te zetten. Fijn dat de minister mee wil denken.

De **voorzitter**:

Voordat we naar het laatste blok gaan, heb ik nog even een vraag en een mededeling. Onze ondersteunde staf is weer zo flexibel geweest om te zeggen: tot 17.00 uur, daar doen we ook wel aan mee. Dat kan gelukkig. Heel veel dank daarvoor, want 16.00 uur gaan we niet halen. Ik weet dat deze minister zich ook graag flexibel opstelt, maar dan moet dat wel mogelijk zijn. Ik kijk dus even naar de minister. Is er een mogelijkheid om uit te lopen tot 17.00 uur?

Minister **Van Weel**:

Ik ben niet op reis en de koning heeft mij ook niet ontboden, dus dan hoor ik nergens anders te zijn dan hier.

De **voorzitter**:

Dat is fijn. Ik denk dat we 17.00 uur wel moeten halen. Dan gaan we nu naar het laatste blokje.

Minister **Van Weel**:

Ik vind 16.00 uur ook nog steeds goed, hoor.

De **voorzitter**:

Dat zou een prestatie zijn. Ik ga voor 16.00 uur, maar mocht dat niet lukken, dan hebben we tot 17.00 uur.

Minister **Van Weel**:

Ik denk dat we een heleboel al gehad hebben, ook rondom de Wwke, maar ik loop nog even specifiek dingen langs, bijvoorbeeld de verhouding tot de

Aanpak vitaal. Ik heb in het begin gezegd hoe die twee zich tot elkaar verhouden, namelijk dat het voor de bedrijven en entiteiten die de Wwke ingaan, naadloos aansluit, maar dat ze nu een wettelijke verplichting hebben. Voor de rest van de entiteiten loopt de Aanpak vitaal gewoon door.

Hoe voorkomen we overlap en versnippering binnen de Wwke en hoe hebben we een duidelijk samenhangend stelsel? Dat was een vraag van mevrouw Zwinkels. Als coördinerend bewindspersoon voel ik me verantwoordelijk voor de bescherming van de vitale infrastructuur. Ik zal dus kijken naar de samenhang tussen verschillende sectoren. De vakministers zijn de bevoegde autoriteit en moeten in principe zelf vanuit hun beleidsverantwoordelijkheid de sectoren bedienen, want zij hebben de kennis en expertise van de sector die ik niet in alle gevallen heb. Ik denk dat het samenspel tussen die twee, dus wel een nationale samenhang en toch een sectorspecifieke aanpak, het beste model is. Dat sluit ook meteen aan op de vraag van mevrouw Zwinkels hoe je voorkomt dat ze op eilandjes gaan werken. Deels vind ik eilandjes prettig, want daar kan men de diepte in qua kennis en expertise, maar er moeten ook bruggen geslagen worden tussen de eilandjes. Daarvoor ben ik dan weer en namens mij de NCTV.

Hoe verhouden de nationale risicobeoordeling en de risicobeoordeling door kritieke entiteiten zich tot elkaar? De nationale risicobeoordeling voor de Wet weerbaarheid kritieke entiteiten wordt per sector uitgevoerd door de vakminister en gaat in op de risico's van een bepaalde sector. De risicobeoordeling van de kritieke entiteit zelf volgt daarna en die gaat weer in op de risico's die specifiek zijn voor die organisatie. Het gaat dus een categorie specifieker naarmate je dichterbij komt. De minister van IenW maakt bijvoorbeeld een risicobeoordeling voor de sector luchtvaart in zijn geheel en daarbinnen maken de kritieke entiteiten dan weer een eigen risicobeoordeling die ze kunnen gebruiken voor de specifieke risico's voor hun entiteit en organisatie. Die bouwt voort op wat de minister sectoraal heeft neergelegd.

Hoe voorkom je dat die beoordelingen los van elkaar plaatsvinden? Dat zit 'm in de volgordelijkheid. Eerst heb je de sectorale risicobeoordeling en de specifieke risicobeoordelingen van de entiteiten zelf sluiten daarop aan. Daarbij moeten ze natuurlijk wel samenwerken, want anders mis je in de sectorale beoordeling weer elementen die uiteindelijk toch een rol gaan spelen bij de lokale beoordeling.

Hoe verhoudt de uitvoeringsstrategie voor de Wwke zich tot de nationale strategie, die ook nog moet worden opgesteld? Ook dat is een vraag van mevrouw Zwinkels. De uitvoeringsstrategie zal ik vaststellen samen met de vakministers en die bevat strategische doelstellingen en prioriteiten om de gehele weerbaarheid te vergroten. Dat is dus eigenlijk de stip op de horizon voor het geheel. Daaronder hangen de sectorale risicobeoordelingen en daaronder dan weer de organisatiespecifieke. Het is dus een boom die zich vertakt onder hetzelfde bladerdak.

Mevrouw Kathmann vroeg hoe alle entiteiten zich naar mijn verwachting met zo'n vitaalbeoordeling identificeren. Zien we ook het risico dat er organisaties zijn die de vitaalbeoordeling niet doen en er daarom niet van op de hoogte zijn dat ze onder deze wet vallen? Dat hoeft niet in het geval van de Wwke, want ze worden gewoon aangewezen. Een kritieke entiteit hoeft dus niet zelf te bepalen of die kritiek is en of die onder de wet valt. Het is juist aan de vakministers om kritieke entiteiten aan te wijzen op basis van de risicobeoordeling en de afweging van de criteria. Een aangewezen entiteit -- dat is anders dan bij de Cyberbeveiligingswet -- wordt altijd direct geïnformeerd door de vakminister en ook vooraf geïnformeerd over de mogelijke aanwijzing.

Hoe snel hebben we alle entiteiten in kaart? Gaan we ze allemaal zo ver krijgen om die beoordeling in te vullen? Zoals ik zei, kunnen ze dat niet zelf doen. De eerste aanwijzingen door vakministers zullen binnen een maand na de inwerkingtreding plaatsvinden. Er kunnen altijd weer ontwikkelingen zijn, technologisch, geopolitiek of anderszins, waardoor je in een later stadium alsnog aanvullende entiteiten zou willen aanwijzen. Die ruimte biedt de wet ook. Ik hoef ze dus ook niet aan te schrijven. Alle kritieke entiteiten krijgen bericht van de bevoegde vakminister. In die zin weten ze vanaf dat moment waar ze aan toe zijn. Daar worden ze vooraf over geïnformeerd.

Hoe ondersteunen we de kritieke entiteiten bij het versterken van hun weerbaarheid? Gebeurt dat bijvoorbeeld via richtsnoeren? Dat was een vraag van mevrouw Zwinkels. Dat loopt via de vakministers. Zij geven advies en zorgen voor de uitwisseling van informatie, maar verlenen ook bijstand. De NCTV ondersteunt weer de vakdepartementen en wij nemen de sectoroverstijgende acties en initiatieven op, zoals de afhankelijkhedenanalyses tussen sectoren. Voor het digitale terrein hebben we natuurlijk het NCSC. Daar hebben we het al eerder over gehad. De inlichtingen- en veiligheidsdiensten helpen met relevante dreigingsinformatie binnen de kaders die zij daarvoor hebben.

Hoe komen we aan de schatting van die 500? Dat aantal is met name gebaseerd op het huidige aantal vitale aanbieders en op de nieuwe sectoren waarin nu nog geen vitale aanbieders zijn aangemerkt, bijvoorbeeld de sector gezondheidszorg en de sector productie, verwerking en distributie van levensmiddelen. Zoals ik zei, is dit uiteindelijk aan de vakministers, maar op basis daarvan zijn wij tot de 500 gekomen.

Hoe borgen we dat de kennis- en informatiedeling tussen vakministers en kritieke entiteiten op orde is? Ook dat was een vraag van mevrouw Zwinkels. Tijdig informeren bij dreigingen is absoluut van belang. De basis hiervoor is de structurele en intensieve informatie-uitwisseling. Daarom werken we, een, aan een informatie- en waarschuwingssysteem, om informatiedeling te faciliteren, en, twee, aan een veilig platform en aan regulier contact tussen de kritieke entiteiten, de vakdepartementen en de veiligheidsdiensten. Ten derde kijken we naar afspraken rondom sectortafels, waar we ook de

inlichtingendiensten kunnen laten aanschuiven, bijvoorbeeld om een algemeen dreigingsbeeld te geven: wat kunt u nou verwachten van statelijke actoren of criminele samenwerkingsverbanden?

Hebben we inmiddels met de Europese Commissie gesproken over het borgen van de informatie-uitwisseling, de vertrouwelijkheid en de betrouwbaarheid? Dat zijn natuurlijk ontzettend belangrijke randvoorwaarden voor het uitwisselen van informatie. Het Nationaal Crisiscentrum is voor mij het nationaal aanspreekpunt voor grensoverschrijdende incidenten. Daarnaast zit de NCTV in de Europese expertgroep voor de weerbaarheid van kritieke entiteiten, de Critical Entities Resilience Group. In dit gremium brengt de NCTV dit vraagstuk regelmatig onder de aandacht van de Europese Commissie.

Hoe zorgen we ervoor dat de verplichtingen onder deze wet proportioneel zijn, ook voor kleinere ondernemers en entiteiten? De proportionaliteit is hierbij een van de uitgangspunten en is daarom risicogebaseerd, net als bij de Cyberbeveiligingswet. Iedere organisatie moet dus maatregelen nemen die passend zijn bij die organisatie, die in verhouding zijn en evenredig zijn. Dat maakt dus wel dat het maatwerk is, ook tussen de verschillende sectoren. Gezondheidszorg is namelijk echt iets anders dan de productie van levensmiddelen of bedrijven die iets meer richting de vitale dienstverlening en de hightech zitten. Ik ben al een paar jaar bezig met weerbaarheid. Als je spreekt met bedrijven in sectoren, dan blijkt juist heel vaak dat zij heel goed weten tegen welke risico's zij zich moeten wapenen. De overheid hoeft daar vaak niet heel veel aan toe te voegen.

In antwoord op de heer Vermeer kan ik hier nog zeggen dat ik uiteraard niet verantwoordelijk ben voor de voedselketen, maar die is natuurlijk wel van cruciaal belang voor Nederland. Voedselzekerheid is een opgave waar we elke dag aan werken. De Wwke draagt daar naar mijn mening aan bij door ook deze vitale sector onder die wet te laten vallen.

Op de evaluatietermijn ben ik al ingegaan.

Krijgen wij een boete voor het niet tijdig implementeren van de CER-richtlijn? Ik hoop het niet, zeg ik daar maar op voorhand bij, maar de Europese Commissie is wel een inbreukprocedure tegen Nederland gestart. We zitten nu echt nog in de eerste administratieve fase. Daarna zou de Commissie kunnen besluiten om bij het Europese Hof van Justitie een zaak aanhangig te maken. Dat zou kunnen leiden tot een boete, maar inmiddels zijn we zo ver in het wetgevingstraject -- zoals ik al zei, kunnen wij ook goed onderbouwen waarom wij zijn begonnen met het leggen van een goed fundament onder deze wet voordat we die behandeld hebben -- dat ik ervan uitga dat dat goed gaat. We zijn echt niet het enige land dat achterloopt of de richtlijn nog niet volledig heeft geïmplementeerd. Onder andere Frankrijk en Spanje zijn daar ook nog mee bezig.

Voorzitter. Ik denk dat ik in mijn eerste termijn dan alleen nog de amendementen heb.

De **voorzitter**:

Dan kijk ik even naar de Kamerleden aan de linkerkant om te zien of dat klopt. Ik zie dat er geknikt wordt, behalve natuurlijk door de heer Van den Berg. Ik had ook niet anders verwacht. Meneer Van den Berg.

De heer **Van den Berg** (JA21):

Ik durf bijna niet meer, voorzitter, maar het zijn maar korte vragen. Het Cyberbeveiligingsbesluit staat nu nog als concept in de interne stukken op Parlis. Wat voor status heeft dat document nu? Is het nog hetzelfde als het concept dat toen naar de Kamer is gestuurd, zijn er nog wijzigingen in aangebracht of komen er nog wijzigingen? Daar ben ik wel benieuwd naar.

Laat ik mijn vragen maar gelijk clusteren. Ik heb nog een openstaande vraag over in hoeverre kwantumencryptie wordt meegenomen, zowel bij kritieke entiteiten als in de Cyberbeveiligingswet.

Dan de laatste. Ik las dat de kosten voor de overheid structureel oplopen tot zo'n 83 miljoen euro vanaf 2028. Ziet de minister nog mogelijkheden om daar meer efficiëntie in aan te brengen?

Minister **Van Weel**:

In reactie op uw eerste vraag: ja, die versie is nog actueel. Het document ligt nu bij de Raad van State voor advies. Dat is de laatste versie.

Wat betreft kwantumencryptie: deze wetten zijn juist technologieonafhankelijk, om ruimte te houden voor technologische ontwikkelingen, zodat we niet een wet hebben waarin kwantum niet wordt genoemd, maar AI wel, en we over drie jaar weer een nieuwe wet moeten maken. De wet dekt dat volledig, maar uiteindelijk zul je het in de uitvoering daarover moeten hebben. 83 miljoen euro vind ik een koopje, moet ik zeggen, voor een zeer omvangrijke wet, zeker als u hoort hoeveel verschillende actoren erbij betrokken zijn, van toezichthouders tot instanties zoals het NCSC. We gaan naar een enorme toename van entiteiten, dus ik voorzie weinig mogelijkheden, maar er is in ieder geval dekking voor het genoemde bedrag.

De **voorzitter**:

Dan kijk ik nog een keer naar de Kamerleden aan de linkerkant. Alle vragen zijn beantwoord. Dan brengt ons dan bij de tweede termijn van de zijde van de Kamer. O nee, eerst nog de amendementen. Excuses. Ik kijk toch weer naar de minister.

Minister **Van Weel**:

De ingediende amendementen, zeg ik daarbij. Ik heb er drie bij de Cyberbeveiligingswet: twee van mevrouw Kathmann en een van mevrouw El Boujdaini. Bij de Wwke heb ik er ook drie: twee van mevrouw Kathmann en een van mevrouw Faber.

Ik begin met het amendement op stuk nr. 12 (36764) van mevrouw Kathmann. Die gaat over het overhevelen van de verplichting naar de wet. Ik geef u twee varianten. Het vierde lid van het amendement, zoals dat er nu staat, voorziet in de inspanningsverplichting voor de vakminister; dat vind ik moeilijk. Daarmee verschuift de verantwoordelijkheid volledig naar de overheid. Ik noemde het net al even in mijn eerste termijn: ik wil investeringen niet compleet derisken. Ik vind dat leveranciers en entiteiten op dat gebied ook een eigen verantwoordelijkheid hebben te nemen. We hebben natuurlijk al de nadeelcompensatie en de Algemene wet bestuursrecht, die, denk ik, ook in dit geval heel goed toepasbaar zijn. Met het vierde lid moet ik het amendement dus ontraden, maar zonder het vierde lid geef ik het oordeel Kamer.

De **voorzitter**:

Dan pas ik het amendement aan. Ik maak er dan gewoon twee amendementen van: één zonder lid vier en één met alleen lid vier. Ik pas het dus aan zoals u zegt. Excuses voor de verwarring.

Minister **Van Weel**:

Het amendement met alleen het vierde lid geef ik bij dezen het oordeel ontraden, om de reden die ik net heb genoemd. Dat hoeft u dus niet opnieuw in te dienen.

Dan het amendement op stuk nr. 13 (36764) over de voorhangprocedure voor de uitwerking van de zorgplicht. Ik heb hier eerder al iets over gezegd. Zeker omdat hier toekomstige wijzigingen mee bedoeld worden, geef ik dit amendement oordeel Kamer.

Dan het amendement op stuk nr. 14 (36764) van mevrouw El Boujdaini. Met referte aan de discussie we net hebben gehad, ontraad ik dit amendement. Ik ben gaarne bereid om mee te denken over een motie die materieel regelt

wat u wilt, maar niet via de wettelijke plicht op basis van de Cyberbeveiligingswet zelf.

Mevrouw **El Boujdaini** (D66):

Als het amendement wordt aangepast, is er dan wel de mogelijkheid dat het oordeel Kamer krijgt? Het gaat mij er namelijk heel erg om dat er een wettelijke grondslag komt, zodat -- ik herhaal mezelf misschien ook wel -- het lokale bestuur informatie kan krijgen, niet alleen over verschillende incidenten, maar bijvoorbeeld ook over wat überhaupt de kritieke entiteiten zijn. Over die informatie beschikken zij namelijk niet. Er staat ook niet in de wet dat zij die informatie kunnen krijgen van het NCSC. Op de vragen vanuit de Kamer heeft het kabinet namelijk geantwoord dat er inderdaad geen wettelijke grondslag voor is dat het NCSC dit soort informatie mag delen. Ik stel dus toch de vraag of er nog een mogelijkheid is om het amendement hier en daar wat aan te passen, zodat het dan misschien toch wel oordeel Kamer krijgt.

Minister **Van Weel**:

Ik ben bang van niet. Dat zit 'm in het fundamentele aspect dat deze wet ziet op hoe wij omgaan met cyberbeveiligingsincidenten in Nederland. Dat heeft in een heleboel gevallen helemaal niets te maken met de fysieke openbare orde. Het feit dat er zich dus een essentiële entiteit bevindt in Amsterdam -- dat zijn er wel honderd in de vorm van IT-bedrijven rondom Amsterdam -- heeft niks te maken met de openbare orde en veiligheid in Amsterdam. Er is in dit opzicht dus geen enkele relatie met de taak van de burgemeester. Het hoofdkantoor van Odido is geen bedreiging. Nou ja, dat kan het worden. Dan vraag je aan mensen van het NCSC, van het CSIRT, om elke keer de afweging te maken of dit nu een incident is bij een kritieke entiteit die ten eerste überhaupt iets te maken heeft met openbare orde en veiligheid. Dat kost mij al capaciteit, want die capaciteit zit daar niet. Dat is niet hun werk. Ten tweede vraag je die dan om de afweging te maken om een lijntje te leggen met het lokale bestuur. Maar ik heb die lijntjes veel liever via de reguliere lijnen die ik heb voor openbare orde en veiligheid. Daar komt de NCSC-informatie vaak wel binnen. Mij bereikt het namelijk wel op het moment dat zoiets speelt. Daarvoor heb ik dan weer geen wettelijke grondslag in de Cyberbeveiligingswet nodig. Dat kunnen we dan gewoon doen via de nationale crisisstructuur. Dat voelt voor mij fijner, want dan word ik gebeld door een burgemeester en weet ik ook waarover het gaat. Als het NCSC daarin zelf een afweging maakt, al dan niet op basis van de juiste gronden, wordt het rommelig, vandaar dat ik dus weinig mogelijkheden zie in dit amendement, maar heel veel in een motie die de facto zorgt voor wat u wilt, namelijk dat ik op het moment dat er iets is wat effect heeft op de openbare orde bij mijn gemeente, daarover word geïnformeerd.

Mevrouw **El Boujdaini** (D66):

Dan overweeg ik het amendement in te trekken en zal ik kijken naar een motie voor straks, in de tweede termijn.

Minister **Van Weel**:

Dan de drie amendementen bij de Wwke.

Het amendement op stuk nr. 9 (36765) van mevrouw Faber, over het vervallen van de grondslag om extra organisaties aan te wijzen, ontraad ik met het oog op de toekomst. Kwantum en crypto werden al even genoemd. Stel je voor dat wij hier een nieuwe kritieke entiteit krijgen, die juist ziet op dat vlak, dat cruciaal wordt voor onze nationale veiligheid in de toekomst. Dan moeten we extra organisaties kunnen toevoegen. Dat hebben we nu dus specifiek voor Nederland gedaan waar het gaat om het keren en het weren van water, juist vanwege de specifieke situatie in Nederland. Ik denk dus dat er altijd aanleiding kan zijn om toch extra organisaties onder de Wwke te gaan brengen. Daar voorziet deze grondslag in. Ik wil daarbij opmerken dat ik het dus ook geen nationale kop vind, omdat we gebruikmaken van een expliciete voorziening die door de wet wordt gegeven. Het is niet iets wat we erbij verzinnen.

Mevrouw **Faber** (PVV):

Wat de minister nu noemt, is in feite gewoon een instrument dat al onder de sectoren valt. Daar is dus in feite al in voorzien. Stel dat er nou een entiteit komt waarvan u zegt: dat is iets nieuws. Dan zou u altijd bijvoorbeeld een spoedwet kunnen indienen. De Kamer hier is daar dol op, dus volgens mij moet dat dan heel snel kunnen.

Minister **Van Weel**:

Nou, daar hebben wij wat andere ervaringen mee. Er gaat ook niks mis als we deze grondslag behouden om in voorkomend geval heel makkelijk en snel over te kunnen gaan tot zo'n aanwijzing. Ik denk dat we nu niks doen wat valt buiten de orde van deze wet, raar is of leidt tot extra inspanningen. Ik behoud die dus graag, vandaar dat ik het ontraad.

Mevrouw **Faber** (PVV):

Ik kan er wel op reageren. Kijk, ik zie dat anders. Het is toch wel prettig om als parlement de controle te houden over de entiteiten die toegevoegd

moeten worden. Als echt de nood aan de man is, weet ik wel dat, zoals we ook hebben gezien met bijvoorbeeld de coronamaatregelen, men heel snel kan acteren als dat moet.

Minister **Van Weel**:

Wij hangen alles voor. Dat hebben we net ook afgesproken. In die zin komt het sowieso in enige vorm langs uw Kamer, ook als het niet per wet is.

Dan het amendement op stuk nr. 10 (36765) van mevrouw Kathmann. Dat is mutatis mutandis hetzelfde.

De **voorzitter**:

Dus hier haal ik de inspanningsverplichting eruit en dan krijgt het oordeel Kamer. Er komt dan een apart amendement waar de inspanningsverplichting in staat en dat amendement wordt dan ontraden.

Minister **Van Weel**:

Ik had het niet beter kunnen verwoorden, voorzitter.

Dan het amendement van mevrouw Kathmann op stuk nr. 11 (36765) over de voorhangprocedure. Daar geldt hetzelfde voor als voor het andere. Omdat het ziet op toekomstige wijzigingen geef ik dat oordeel Kamer.

De **voorzitter**:

Dat brengt ons wel bij de tweede termijn van de Kamer. Dan kijk ik gelijk naar de heer Van den Berg van JA21.

De heer **Van den Berg** (JA21):

Ik weet niet hoe de rest erin staat, maar is er wellicht ruimte voor een hele korte sanitaire stop?

De **voorzitter**:

Nou, ik denk dat het handig is …

De heer **Van den Berg** (JA21):

In reactie op wat mevrouw Faber buiten de microfoon zegt: die inschatting laat ik voor haar!

De **voorzitter**:

Meneer Van den Berg, ik denk dat het handig is om nu heel snel de tweede termijn te doen en dan hebben we sowieso even een kleine schorsing.

De heer **Van den Berg** (JA21):

Kunnen we anders de sprekersvolgorde even omwisselen?

De **voorzitter**:

Oké. Mevrouw Faber. Uw tweede termijn? Nee, u maakt daar geen gebruik van. Dan mevrouw Martens-America.

Mevrouw **Martens-America** (VVD):

Dank, voorzitter. Dank aan de minister. Wij zijn blij met de toezeggingen met betrekking tot de evaluatietermijn, dat er nu dus gekeken gaat worden naar twee jaar. Dank voor de beantwoording.

De **voorzitter**:

Mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Dank, voorzitter. Ik wil nog een motie indienen in de tweede termijn. Die is alleen nog onderweg, dus misschien kan ik straks aan de beurt komen?

De **voorzitter**:

Ja. Dan mevrouw El Boujdaini.

Mevrouw **El Boujdaini** (D66):

Ik wil graag twee moties indienen.

Ik begin bij de motie over het versterken van de informatiepositie van burgemeesters en veiligheidsregio's. Ik zal 'm even oplezen.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de burgemeester op grond van de Gemeentewet verantwoordelijk is voor de handhaving van de openbare orde binnen de gemeente en dat de voorzitter van de veiligheidsregio is belast met crisisbeheersing op regionaal niveau;

constaterende dat cyberincidenten bij organisaties in de gemeente, zoals ziekenhuizen, energiebedrijven of vervoerders, directe gevolgen kunnen hebben voor de openbare orde;

verzoekt de regering de informatiepositie van burgemeesters en voorzitters van de veiligheidsregio's te versterken bij cyberincidenten met gevolgen voor de openbare orde en hiervoor indien nodig een grondslag te creëren voor informatiedeling met burgemeesters en voorzitters van de veiligheidsregio's,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid El Boujdaini.

Zij krijgt nr. 15 (36764).

De Cbw heeft dossiernummer 36764. Betreft dit inderdaad de Cbw?

Mevrouw **El Boujdaini** (D66):

Ja, dit gaat om de Cbw.

De **voorzitter**:

Dan noteren we bij deze motie dossiernummer 36764.

Mevrouw **El Boujdaini** (D66):

Oké.

Dan een tweede motie, ook over de Cbw, dus 36764. Deze motie gaat over een plan of een routekaart voor een cybersecuritystelsel voor het Caribisch deel van het Koninkrijk.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat het Caribisch deel van het Koninkrijk ook te maken heeft met cyberdreigingen en digitale bescherming en weerbaarheid daar ook cruciaal is;

constaterende dat de Veiligheidsstrategie van het Koninkrijk der Nederlanden een goed begin is, maar nog niet toereikend genoeg;

verzoekt het kabinet aan een concreet plan of een routekaart te werken om te komen tot een cybersecuritystelsel voor het Caribisch deel van het Koninkrijk dat zo veel mogelijk aansluit bij het niveau van digitale bescherming en weerbaarheid in Europees Nederland, en dit samen met het Caribisch deel te doen,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door de leden El Boujdaini en Kathmann.

Zij krijgt nr. 16 (36764).

Mevrouw **El Boujdaini** (D66):

Dan wil ik de minister nog graag bedanken voor de beantwoording en ook voor de suggestie en het meedenken over de motie.

De **voorzitter**:

Dan is het woord aan mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Dank u wel, voorzitter. Ik wil beginnen met het bedanken van de minister voor de beantwoording en de diverse toezeggingen. We hebben hier vandaag een goed debat gehad.

Ik heb tot slot één motie en die gaat over de ketensamenwerking tussen bedrijven.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat digitale weerbaarheid niet alleen afhangt van de beveiliging van afzonderlijke organisaties, maar ook van de samenwerking en kennisdeling binnen ketens;

overwegende dat cyberdreigingen zich snel ontwikkelen en dat binnen ketens een gedeeld belang bestaat om de digitale beveiliging op orde te hebben;

overwegende dat kleinere bedrijven baat kunnen hebben bij betere toegang tot dreigingsinformatie en de geleerde lessen;

verzoekt de regering in kaart te brengen hoe de uitwisseling van dreigingsinformatie en geleerde lessen binnen ketens kan worden versterkt,

in het bijzonder zodat ook kleinere bedrijven daarvan beter kunnen profiteren, en de Kamer hierover te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Zwinkels.

Zij krijgt nr. 17 (36764).

Dit is ook 36764, hè? Dit gaat over de Cbw?

Mevrouw **Zwinkels** (CDA):

Ja, dit gaat over de Cyberbeveiligingswet.

De **voorzitter**:

Ja, dat klopt. Ik kijk even of de heer Van Dijk behoefte heeft ... Nee, hij heeft geen behoefte aan een tweede termijn.

Dan kijk ik naar de heer Van den Berg, want ik kan ook, hè. Zeg het maar.

De heer **Van den Berg** (JA21):

Nee, we zijn nu toch bezig, voorzitter. Allereerst dank aan de minister voor alle uitleg en de toelichting op alle gestelde vragen. Het waren er inderdaad behoorlijk veel. Het is ook fijn om in dit debat een keer met minister Van Weel te sparren.

Het was al even te zien: dit zijn de moties en amendementen die nog niet zijn ingediend. In ieder geval is wel helder waar de minister heen wil en waar wel en niet draagvlak voor is. Wij zullen onze amendementen en moties nog indienen, maar dan natuurlijk wel rekening houdend met de discussie die we hier met elkaar hebben gevoerd. Een discussie die overigens zeer constructief was. Laat ik het daar voor nu bij houden.

Dank u wel.

De **voorzitter**:

Dan draag ik het voorzitterschap even over voor de tweede termijn van het lid Kathmann van GroenLinks-Partij van de Arbeid.

Voorzitter: Van den Berg

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ook ik wil in de eerste plaats de minister van harte danken voor de zorgvuldige beantwoording. Het is inderdaad heel helder op welke lijn de minister zit.

Ik heb nog wel een aantal moties. De eerste betreft dossiernummer 36764.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de Cyberbeveiligingswet een zorgplicht en een meldplicht introduceert om cyberveiligheidsrisico's te voorkomen en beheersen;

overwegende dat een grootschalig datalek directe gevolgen heeft voor slachtoffers wier persoonsgegevens worden buitgemaakt, zoals bij de Odidohack en het lek bij het bevolkingsonderzoek baarmoederhalskanker;

overwegende dat er nog geen wettelijk kader bestaat voor hoe individuele slachtoffers geholpen en geïnformeerd moeten worden in de nasleep van een grootschalig datalek;

verzoekt de regering om een wettelijke nazorgplicht te onderzoeken voor incidenten waarin op grote schaal persoonsgegevens worden gelekt, met als doel om de rechten van individuele slachtoffers en de plichten voor de getroffen instantie(s) in de wet vast te leggen;

verzoekt de regering om dit onderzoek uiterlijk in Q3 van 2026 af te ronden en de Kamer hierover te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 18 (36764).

Mevrouw **Kathmann** (GroenLinks-PvdA):

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten een meldplicht introduceren waarvoor een meldloket wordt ingericht;

overwegende dat entiteiten baat hebben bij één centraal en overzichtelijk meldloket, dat bruikbaar is voor alle soorten meldingen die volgen uit nationale en sectorale wetgeving;

verzoekt de regering om één centraal meldloket in te richten waarbinnen alle relevante soorten meldingen gedaan kunnen worden;

verzoekt de regering om de Kamer in Q4 van 2026 te informeren over de inrichting van het centrale meldloket,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 19 (36764).

Mevrouw **Kathmann** (GroenLinks-PvdA):

Deze motie wil ik mogelijk aanhouden of intrekken, want de minister heeft hier een uitgebreide toezegging over gedaan. Alleen wil ik wel weten of die toezegging echt is bedoeld inclusief alle meldmogelijkheden die nu al gelden voor bijvoorbeeld ... Ik weet niet precies hoe het heet; is het Ceveso-wetgeving of Seveso-wetgeving? Volgens mij valt het onder IenW, de AVG en andere sectorale regels. Gaat het echt over één loket dat alles bundelt, zodat straks op één plek alles samen kan komen? Als dat de toezegging is -- het was al een mooie toezegging -- dan zou dat helemaal mooi zijn. Het zou mooi zijn als daar ook een termijn aan verbonden kon worden, want dan kan ik die motie gewoon intrekken.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat het kabinet heeft ingeschat dat tussen de 7.550 en 8.100 entiteiten onder de Cyberbeveiligingswet zullen vallen, en 500 entiteiten onder de Wet weerbaarheid kritieke entiteiten;

overwegende dat het kabinet vooralsnog uitgaat van het vrijwillig uitvoeren van een nationale vitaalbeoordeling door deze entiteiten, waaruit blijkt of ze aan de wetgeving moeten voldoen;

verzoekt de regering om organisaties die vermoedelijk aan de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten moeten voldoen, proactief op te roepen om de vitaalbeoordeling uit te voeren en hierop toe te zien;

verzoekt de regering om dezelfde organisaties gelijktijdig te wijzen op relevante informatie en deadlines voor organisaties die als entiteit worden aangemerkt,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 20 (36764).

Mevrouw **Kathmann** (GroenLinks-PvdA):

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat er binnen vier tot vijf jaar na de inwerkingtreding van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten een evaluatie wordt gedaan naar de effectiviteit van de wetten;

overwegende dat dit een logisch moment is om te bezien of er aanvullende aanpassingen wenselijk en mogelijk zijn, zoals het onderbrengen van zaken uit de lagere regelgeving op het niveau van de wet, en het uitbreiden van de reikwijdte naar de Caribische delen van het Koninkrijk;

verzoekt de regering om bij de evaluatie van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten te bezien of, en zo ja, hoe, de wetten aangepast kunnen worden zodat verplichtingen uit de lagere regelgeving zo veel mogelijk op het niveau van de wet zijn geregeld en de reikwijdte van de wetten binnen een redelijke termijn wordt uitgebreid naar heel het Koninkrijk,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 21 (36764).

Voorzitter: Kathmann

De **voorzitter**:

Dan heeft iedereen volgens mij zijn tweede termijn achter de rug. Ik kijk even naar de minister met de vraag hoeveel tijd er nodig is. O, de heer Van den Berg heeft toch nog even iets toe te voegen aan zijn tweede termijn.

De heer **Van den Berg** (JA21):

Jazeker. Ik had van tevoren al even gecheckt of wij de moties eventueel later nog kunnen indienen. Er was even een misverstand. Ik moet mijn mooie boekje dus gaan opofferen en de moties eruit scheuren. U heeft er een voor me? Nee, daar komt natuurlijk nog de steun uit. Ik ga het toch even zo doen. We zijn creatief.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat entiteiten in de praktijk tegelijk onder de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten kunnen vallen en daardoor met meerdere bevoegde autoriteiten, audits, informatieverzoeken en bewijssets te maken kunnen krijgen;

overwegende dat effectieve weerbaarheid vraagt om zo min mogelijk dubbel werk en dat toezichtlast niet onnodig mag afleiden van feitelijke beveiligings- en weerbaarheidsmaatregelen;

verzoekt de regering om voor entiteiten die onder beide wetten vallen uit te werken dat één gecoördineerd dossier, één auditkalender, één zo veel mogelijk herbruikbare bewijsset en één coördinerend aanspreekpunt het uitgangspunt zijn, en dat dubbele informatieverzoeken alleen plaatsvinden indien dat aantoonbaar noodzakelijk is,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Van den Berg.

Zij krijgt nr. 22 (36764).

De heer **Van den Berg** (JA21):

Dan moet ik wel de achterkant nog even terug hebben, want daar staat ook nog een motie op. Prachtig, dit.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat voor overheidsorganisaties de uitwerking van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten kan samenlopen met de BIO (Baseline Informatiebeveiliging Overheid) en ENSIA (Eenduidige Normatiek Single Information Audit);

overwegende dat dubbele verantwoordings-, audit- en bewijsstructuren capaciteit wegnemen die juist nodig is voor feitelijke weerbaarheid;

verzoekt de regering om bij de uitwerking van lagere regelgeving, handreikingen en toezichtpraktijk onder de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten voor overheidsorganisaties expliciet te borgen dat verplichtingen, bewijslasten, auditlogica en verantwoordingsinformatie zo veel mogelijk worden geharmoniseerd met BIO en ENSIA, en de Kamer hierover vóór de inwerkingtreding te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Van den Berg.

Zij krijgt nr. 23 (36764).

De heer **Van den Berg** (JA21):

Dan heb ik de achterkant van die andere motie nog even nodig. Creativiteit, maar het komt goed.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat artikel 34 van de Wet weerbaarheid kritieke entiteiten een ruime vertrouwelijkheidsregeling bevat en dat bij of krachtens de Wwke leveranciersmaatregelen kunnen worden getroffen die diep ingrijpen in bedrijfsvoering, eigendom en continuïteit;

overwegende dat de Kamer ook op deze onderdelen haar controlerende taak moet kunnen uitoefenen zonder operationele belangen, kwetsbaarheden of veiligheidsbelangen te schaden;

verzoekt de regering om de Kamer vanaf de inwerkingtreding van de Wwke halfjaarlijks vertrouwelijk en geaggregeerd te informeren over de toepassing van artikel 34 Wwke in zwaarwegende gevallen en over de toepassing van leveranciersmaatregelen, met in elk geval informatie over aantallen, betrokken sectoren, de algemene aard van het risico en de stand van eventuele bezwaar- en beroepsprocedures,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Van den Berg.

Zij krijgt nr. 12 (36765).

De heer **Van den Berg** (JA21):

Dan zijn we rond. Ik mis wel een beetje het scheureffect.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat entiteiten die onder zowel de Cyberbeveiligingswet als de Wet weerbaarheid kritieke entiteiten vallen met meerdere bevoegde autoriteiten te maken kunnen krijgen en dat in het dossier is gewezen op het risico van meervoudige beboeting voor hetzelfde feitencomplex;

overwegende dat effectieve handhaving niet mag ontaarden in dubbel punitief optreden voor dezelfde feiten en hetzelfde beschermde belang;

verzoekt de regering om bij de uitwerking van samenwerkingsafspraken, handhavingsbeleid en lagere regelgeving te borgen dat voor hetzelfde feitencomplex en hetzelfde beschermde belang niet meer dan één punitieve sanctie wordt opgelegd onder de Cbw en de Wwke, en de Kamer vóór de inwerkingtreding te informeren hoe dit is geborgd,

en gaat over tot de orde van de dag.

De **voorzitter**:

Deze motie is voorgesteld door het lid Van den Berg.

Zij krijgt nr. 24 (36764).

De heer **Van den Berg** (JA21):

Dank. Alles komt weer tot een goed einde.

De **voorzitter**:

Dan kijk ik toch nog één keer naar de heer Van den Berg. Dit was 'm, hè?

De heer **Van den Berg** (JA21):

Jazeker.

De **voorzitter**:

Dan zijn we echt klaar met de tweede termijn van de zijde van de Kamer. Ik kijk heel even hoeveel tijd de minister nodig heeft. We gaan drie minuten schorsen.

De vergadering wordt van 16.08 uur tot 16.14 uur geschorst.

De **voorzitter**:

Achter de schermen is er weer keihard gewerkt om alles klaar te hebben. We wachten niet op de motie op stuk nr. 12 (36765) en de motie op stuk nr. 24 (36764), maar die komen er wel nog aan. Zo kunnen we alvast beginnen met de appreciatie van de moties. Het woord is aan de minister.

Minister **Van Weel**:

Dank, voorzitter. Dank ook aan de leden voor de inbreng in tweede termijn. Ik ga in sneltreinvaart door de moties heen.

De motie op stuk nr. 15 (36764), van mevrouw El Boujdaini, gaat over lokale overheden. Oordeel Kamer.

De motie op stuk nr. 16 (36764) gaat over de routekaart voor het Caribisch deel van het Koninkrijk. Oordeel Kamer.

De motie op stuk nr. 17 (36764), van mevrouw Zwinkels, gaat over de ketensamenwerking. Oordeel Kamer.

De motie op stuk nr. 18 (36764), van mevrouw Kathmann, gaat over de nazorgplicht. Oordeel Kamer, als ik de motie zo mag opvatten dat we het gevraagde betrekken bij de uitwerking van de motie-Rajkowski die op hetzelfde onderwerp ziet.

De **voorzitter**:

Zeker. Vindt u het prettig als ik dat als indiener aanpas in de tekst?

Minister **Van Weel**:

Dat helpt.

De **voorzitter**:

Dank; dan zal ik dat doen.

Minister **Van Weel**:

Dank.

Dan de motie op stuk nr. 19 (36764). Ik was erg scheutig met het centraal meldpunt, maar zo scheutig als u mij hier wil laten zijn, kan ik toch net niet zijn. De reikwijdte die u noemt, wordt te groot. Die gaat over te veel verschillende sectoren heen. We riskeren daarmee een one-size-fits-all waarbij je eerst een kwartier door een belmenu heen moet, omdat het aantal instanties die erachter zitten te breed is. We proberen om er zo veel mogelijk onder te brengen wat echt betrekking heeft op de Cyberbeveiligingswet en de Wwke; ik noemde al twee richtlijnen die we er ook bij onderbrengen. We zullen continu kijken naar het centraliseren, maar gezien de reikwijdte van dit dictum moet ik deze motie helaas ontraden.

De motie op stuk nr. 20 (36764) kan ik oordeel Kamer geven als ik die zo mag interpreteren dat wij "proactief oproepen" niet verstaan als individueel aanschrijven maar als ertoe oproepen via media, social media, webinars et cetera. Voor de Wwke is het sowieso geen probleem, want die organisaties krijgen allemaal al individueel een benadering door de vakminister. Met deze interpretatie: oordeel Kamer.

De **voorzitter**:

Zo kan die geïnterpreteerd worden, zeg ik via de voorzitter.

Minister **Van Weel**:

Dank.

De motie op stuk nr. 21 (36764) gaat over de evaluatie en over bezien welke onderdelen naar wetgeving kunnen. Die motie wil ik oordeel Kamer geven, maar ik wil daarbij wel zeggen dat het deel van het dictum dat zegt "zo veel als mogelijk" niet mijn enige leidende criterium is. Ik zou zeggen "waar nodig en opportuun". Met die tekst kan ik de motie oordeel Kamer geven. Maar het is geen doel op zich om alles vast te leggen in hogere regelgeving, omdat dat ons ook weer vast kan zetten voor toekomstige ontwikkelingen. Als ik de motie zo mag interpreteren, kan deze oordeel Kamer krijgen.

De **voorzitter**:

Ja, dat kan, zeg ik ook weer via de voorzitter. Mevrouw Zwinkels?

Mevrouw **Zwinkels** (CDA):

Het is niet mijn eigen motie, maar ik ben altijd kritisch op ruime interpretaties van moties. Ten aanzien van een punt zoals dit kan ik mij voorstellen dat het belangrijk is dat we de motie in de boeken hebben staan zoals die ook bedoeld is. Ik ga er niet voorliggen, maar vind het hier best wel wezenlijk dat ... Dit zou aangepast kunnen worden, laat ik het zo zeggen.

De **voorzitter**:

Als voorzitter kan ik alleen maar zeggen: dat is genoteerd. Dan denk ik dat het aan de indiener is om even aan te geven of de tekst zal worden aangepast.

Minister **Van Weel**:

Mijn advies voor de aanpassing zou zijn om in plaats van "zo veel mogelijk", "waar nodig en opportuun" te schrijven.

De **voorzitter**:

Dan zegt de indiener dat het aangepast gaat worden.

Minister **Van Weel**:

Dank, voorzitter.

De motie op stuk nr. 22 (36764) krijgt oordeel Kamer.

De motie op stuk nr. 23 (36764): oordeel Kamer.

De motie op stuk nr. 12 (36765): oordeel Kamer.

De motie op stuk nr. 24 (36764): oordeel Kamer. En dat is niet omdat het 16.15 uur is.

De **voorzitter**:

Dan kijk ik even naar mijn linkerzijde. Volgens mij is iedereen tevreden. Ik dank de minister voor de beantwoording, de toezeggingen en de appreciatie van de moties en amendementen. We hebben natuurlijk nog een aantal toezeggingen staan. Die zal ik even met u doornemen.

- Een. De minister van JenV zegt toe een schriftelijk overzicht met de Kamer te delen over de punten in de Cyberbeveiligingswet die nog nader uitgewerkt dienen te worden, inclusief, waar het kan, een vernoeming van termijnen waarop deze uitgewerkt zullen worden.

Dan is nog wel even de vraag binnen welke termijn dat naar de Kamer kan.

Minister **Van Weel**:

Voor de inwerkingtreding. Ik hoop natuurlijk dat dat ergens voor de zomer zal zijn, maar de inwerkingtreding is hier wat mij betreft leidend voor.

De **voorzitter**:

Dan komt daarbij "voor de inwerkingtreding van de wet".

- De tweede. De minister van JenV zegt toe om de Cyberbeveiligingswet binnen twee jaar na invoering van de wet te gaan evalueren, wel na de evaluatie van de betreffende commissie, de regeldruk hierin mee te nemen en de relevante punten voortvloeiend uit de periodieke evaluatie van de Cyberbeveiligingswet die implicaties hebben voor de Wet weerbaarheid kritieke entiteiten mee te nemen in de verdere uitvoering van de Wet weerbaarheid kritieke entiteiten.

- Drie. De minister van JenV zegt toe om de samenwerkingsafspraken die zullen worden gemaakt tussen toezichthouders bij het directeurenoverleg voor de invoering van de Cyberbeveiligingswet met de Kamer te delen en in de Staatscourant te publiceren.

- Vier. De minister van JenV zegt toe schriftelijk terug te komen op de door het lid Faber genoemde casus inzake de Wet weerbaarheid kritieke entiteiten en de afhankelijkheid van het toezicht, bijvoorbeeld in het geval van de kerncentrale.

Wanneer komt dat richting de Kamer?

Minister **Van Weel**:

Voor de zomer.

De **voorzitter**:

Voor de zomer komt dat naar de Kamer.

- Vijf. De minister van JenV zegt toe de vraag over een nazorgplicht voor slachtoffers van cyberaanvallen, gesteld door het lid Kathmann, mee te nemen in de verdere uitwerking van de betreffende motie van het lid Rajkowski.

- Zes. De minister van JenV zegt toe het door het lid Van den Berg gevraagde tijdspad over de uitwerking van de Cyberbeveiligingswet richting Caribisch Nederland mee te nemen in de eerste evaluatie van de wet en aan de staatssecretaris Koninkrijksrelaties de vraag van het lid El Boujdaini, inzake een algemene routekaart voor het cyberbeschermings- en weerbaarheidsniveau van Caribisch Nederland, door te geleiden.

- Zeven. De staatssecretaris Digitale Economie en Soevereiniteit en de minister van JenV zullen in samenwerking voor het eind van het jaar de Kamer informeren over de vragen van het lid Zwinkels inzake gekwalificeerde vertrouwensdiensten en mogelijke alternatieven in gehanteerde werkwijzen hierbij.

Dan knikt ook iedereen. Ik kijk toch nog even naar het lid Kathmann van GroenLinks-Partij van de Arbeid voor de eenloketgedachte. Er was in ieder geval wel een toezegging om één loket te doen, maar dan wel in de bewoording die de minister daaraan heeft gegeven.

Minister **Van Weel**:

Ja.

De **voorzitter**:

Dan zijn we er. Mevrouw El Boujdaini heeft nog een vraag.

Mevrouw **El Boujdaini** (D66):

Ik zat even te denken. Mijn vragen over het Caribisch deel van Nederland zouden kunnen worden ondervangen als mijn motie over die routekaart gewoon wordt aangenomen. Het ligt er even aan. Als die motie wordt

aangenomen, dan hoeft die vraag ook niet meer door de staatssecretaris Koninkrijksrelaties te worden beantwoord.

Minister **Van Weel**:

Ik hoor een stemadvies.

De **voorzitter**:

Ja, dit was een soort campagne voor de motie. We hebben net een campagne achter de rug! Mevrouw Zwinkels.

Mevrouw **Zwinkels** (CDA):

Ik had nog één vraag over een toezegging die ik had gekregen ten aanzien van die samenwerkingsafspraken tussen toezichthouders. Is daar nou wel of niet een termijn aan gekoppeld? Die hoorde ik zojuist niet. Die termijn kan ook zijn "t.z.t., zodra dat gereed is en gepubliceerd kan worden in de Staatscourant".

De **voorzitter**:

Daar staat expliciet bij: voor de invoering van de Cyberbeveiligingswet met de Kamer te delen. Dat is dus voor de invoering van de wet.

Mevrouw **Zwinkels** (CDA):

Prima.

De **voorzitter**:

Volgens mij is dan echt iedereen tevreden. Dan dank ik de minister en iedereen achter de schermen voor de goede zorgen. Ik kijk even naar links, want ik vergeet iets. Wat moet ik nog doen? Volgende week stemmen we over de moties en de week daarop stemmen we over de amendementen en het wetsvoorstel. Ik sluit de vergadering.

Sluiting 16.23 uur.