10
Cybersecuritywet

Aan de orde is de behandeling van:
- **het wetsvoorstel Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet) (34883).**

De **voorzitter**:
Aan de orde zijn de regels ter implementatie van EU-richtlijn 2016/1148, de Cybersecuritywet. Ik moet er als voorzitter op toezien dat in deze zaal Nederlands en geen Engels wordt gesproken, maar ik geloof dat een van de leden, de heer Van Dam, daar ook al een oplossing voor heeft bedacht. Ik denk dus dat dit probleem zich gedurende het debat vanzelf gaat oplossen. Ik heet de minister van Justitie en Veiligheid van harte welkom, net als de leden en iedereen die meekijkt. Ik geef graag als eerste het woord aan mevrouw Buitenweg namens GroenLinks.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, meneer de voorzitter. We spreken vandaag over het omzetten in Nederlandse wetgeving van een Europese afspraak om onze netwerkbeveiliging en informatiebeveiliging te verbeteren. Dat is een belangrijk onderwerp. Het jaarverslag van de AIVD laat zien dat buitenlandse mogendheden en criminele organisaties het gemunt hebben op onze digitale systemen, uit winstbejag of om het democratisch proces te verstoren. En hacks kunnen enorme gevolgen hebben voor elektriciteits- en drinkwatervoorzieningen, voor medische veiligheid, de nationale veiligheid enzovoort.

De minister sprak onlangs over de noodzaak van digitale dijkbewaking en ik kan mij die uitspraak voorstellen. GroenLinks steunt dan ook de Cybersecuritywet, maar we hopen wel dat het kabinet de strekking daarvan ook zelf ter harte neemt. Omdat gister dit onderwerp al uitgebreid aan de orde is geweest bij het Verantwoordingsdebat zal ik het kort houden, maar het is natuurlijk wel echt ernstig dat van alle departementen op dit moment alleen het ministerie van Algemene Zaken en het ministerie van Sociale Zaken en Werkgelegenheid voldoen aan de vereisten van cyberbeveiliging. Hoe ziet de minister nou zijn taak om dit op orde te krijgen?

Met de nieuwe wet worden leveranciers van essentiële diensten verplicht hun ICT-beveiliging op orde te brengen en ernstige cybersecurityincidenten te melden bij de daarvoor aangewezen autoriteiten. Qua opdracht doet de implementatie van deze wet niet onder voor een ander groot project, dat morgen verder zijn beslag krijgt, namelijk de Algemene verordening gegevensbescherming. Maar in vergelijking daarmee is de informatie voor bedrijven summier en soms onduidelijk. Zijn de klachten over onduidelijkheid bij de minister bekend en wat wil hij daaraan gaan doen?

Voorzitter. Bij de uitvoering van de AVG, de Algemene verordening gegevensbescherming, speelt een EU-breed coördinatiemechanisme een grote rol. Dat kan richtlijnen uitvaardigen over hoe de verordening precies geïnterpreteerd moet worden. Daarmee zorgt deze artikel 29-werkgroep voor coherentie op Europees niveau. Zo'n werkgroep ontbreekt bij de Cybersecuritywet, maar zou die ook hier niet een goed idee zijn? Ik vraag de minister of hij ervoor voelt om zich in EU-verband hard te maken voor zo'n mechanisme.

Van verschillende bedrijven heb ik ook hun zorg vernomen over de procedures die gaan gelden. Ik begrijp dat het kan voorkomen dat een cyberincident bij maar liefst drie loketten moet worden gemeld, bijvoorbeeld een datalek met persoonsgegevens bij een groot telecombedrijf. Dat moet gemeld worden bij het Agentschap Telecom als toezichthouder voor de cybersecurity, bij het NCSC omdat het een vitale organisatie betreft en bij de Autoriteit Persoonsgegevens. Is de minister het met mij eens dat dit wel heel erg veel van het goede is en zou er niet voor moeten worden gekozen om één loket aan te wijzen? En dan natuurlijk het liefst het meest voor de hand liggende loket. Het lijkt mij dat dit de slagkracht ten goede komt en de administratieve belasting voor bedrijven zal beperken.

Tot slot. Vanmiddag vergaderde de commissie Economische Zaken over beter aanbesteden. Daarin kwam onder meer aan de orde het besluit van deze minister om het Russische bedrijf Kaspersky in de ban te doen. Ik snap de overweging van de minister heel goed, maar mijn fractie heeft er wel vragen over. Want hoe komt zo'n besluit tot stand? Ik begrijp goed dat sommige analyses geheim moeten blijven omdat het informatie is die via geheime diensten wordt aangeleverd. Maar is de minister zeker van zijn zaak? Is er bewijs of is het besluit genomen op basis van een vermoeden? En is bij het besluit dan ook meegewogen wat dit betekent voor lopende aanbestedingen? Want volgens de collega van de minister is dit niet een zaak voor staatssecretaris Keijzer, maar voor de minister van Justitie. Ik hoop dus van hem een antwoord te krijgen.

Zijn er ook bedrijven waarvan de diensten door de Nederlandse overheid worden ingekocht, die de software nog wel gebruiken? Wat zijn dus nu de eisen op dit gebied en voor wie gelden ze? Klopt het dat C2000 is ontwikkeld door een bedrijf dat in Chinese handen is? En wat vindt u daar dan van? Kortom, GroenLinks en ik denk ook heel veel bedrijven hebben behoefte aan een beleidslijn juist voor de cybersecurity. Dank u wel.

De **voorzitter**:
Hartelijk dank. Dan geef ik het woord aan de heer Alkaya namens de SP.

De heer **Alkaya** (SP):
Veel dank, voorzitter. De afgelopen jaren worden wij steeds meer geconfronteerd met internetaanvallen, zowel gericht op individuen als op belangrijke systemen en diensten waar wij allemaal gebruik van maken. WannaCry leidde vorig jaar tot chaos in de Britse gezondheidszorg, waar ziekenhuizen werden gesloten en operaties werden uitgesteld. In Nederland raakten onder andere ICT-systemen van parkeergarages van Q-Park besmet met ransomware en werden banken meerdere keren geraakt door ddos-aanvallen; vandaag nog ABN AMRO.

Natuurlijk hebben organisaties er primair zelf het grootste belang bij dat zij computersystemen goed beveiligen, maar

er is ook een collectief belang. Daarom is het goed dat het hoofdprincipe van een verplichting om computersystemen goed te beveiligen in de wet staat, nog los van de precieze vorm die die zal aannemen per sector. Maar de reikwijdte van deze wet is helaas vrij beperkt. Alleen vitale diensten en een groep onlinedienstverleners zullen onder deze implementatiewet van een Europese richtlijn vallen. De redenering van de richtlijn is dat problemen bij andere ondernemingen minder grote maatschappelijke gevolgen hebben en daarom zou het niet nodig zijn om deze verplichting ook voor hen te laten gelden.

Op het advies van de Autoriteit Persoonsgegevens om ook andere partijen onder deze wet te laten vallen, antwoordt het kabinet verder dat het Digital Trust Center een belangrijke rol moet spelen in de advisering aan partijen, bijvoorbeeld het midden- en kleinbedrijf. Dat is natuurlijk goed. Er heeft nota bene een SP-motie aan de basis gelegen van het Digital Trust Center, maar is advisering wel voldoende in dezen? Waarom zouden wij geen wettelijke verplichting opnemen om fabrikanten van alle apparaten die aangesloten worden op het internet te verplichten om die apparaten adequaat te beveiligen? In huishoudens worden namelijk steeds meer apparaten op het internet aangesloten, en niet alleen computers, tablets en telefoons, maar ook andere apparaten: koelkasten, televisies en robotstofzuigers. Doordat er geen verplichting is om dit soort apparaten goed te beveiligen en ook beveiligd te houden, met updates, lopen gebruikers niet alleen zelf gevaar, maar dragen ze onbedoeld ook bij aan ddos-aanvallen zoals er vandaag weer een heeft plaatsgevonden.

Dat fabrikanten niet verplicht worden om hun internetapparaten goed te beveiligen, is sterk achterhaald. Om hackers te weren wil de SP minimale veiligheidseisen stellen aan alle internetapparaten, vergelijkbaar met al bestaande milieu-, gezondheids- en veiligheidseisen die aan apparaten worden gesteld. Er ligt ook een aangenomen motie van deze Kamer hierover, waar volgens mij onder andere de naam van D66 onder staat. Ik hoor dus graag waarom er niet voor is gekozen om internetapparaten en andere diensten ook onder deze implementatiewet te laten vallen. Dat lijkt mij een gemiste kans, want de richtlijn streeft naar minimumharmonisatie en de minister had, bij mijn weten, verder kunnen gaan, door in principe alle op het internet aan te sluiten apparaten onder deze implementatiewet te laten vallen. Daardoor had hij ons beter kunnen beveiligen. Na alle incidenten van de laatste tijd — beveiligingslekken, ddos-aanvallen, gehackte camera's en onzekerheid bij burgers over wat er met hun gegevens gebeurt — kan het volgens mij geen kwaad om verdergaande preventieve maatregelen te nemen.

Ten slotte is in de stukken te lezen dat de organisatie die de meldingen over inbraken bij internetdiensten moet verzamelen — excuus, want dat is toch een Engels woord — het Computer Security Incident Response Team, CSIRT, ook een heel mooie afkorting, per Koninklijk Besluit zal worden aangewezen in plaats van per Algemene Maatregel van Bestuur zoals eerst werd voorgesteld. Dit zou zijn om tijdwinst te boeken, omdat wij al te laat zijn met de implementatie van deze Europese richtlijn. Eerlijk gezegd vind ik het niet een supersterk argument dat wij te laat zijn met de implementatie en dat we daarom nu kiezen voor een minder degelijk proces in de aanwijzing van zo'n organisatie, en dat we dat dan nu ook op zo'n manier in de wet vastleggen. Dus vraag ik de minister of hij kan toelichten hoe hij de Tweede Kamer, en overigens ook de Raad van State, wil meenemen in het vervolg van dit proces, als wij niet meer bij wet meegenomen zullen worden.

Veel dank, voorzitter.

De **voorzitter**:
Hartelijk dank. Dan geef ik het woord aan de heer Van Dam namens het CDA.

□

De heer **Van Dam** (CDA):
Voorzitter, dank u wel. Laat ik beginnen met te vertellen dat "CDA" een Nederlandse afkorting is. Het staat voor Christen-Democratisch Appèl. Ook andere afkortingen zal ik waar mogelijk toelichten.

Voorzitter. De meest wezenlijke bijdrage die ik wil leveren aan dit debat over deze wet is een pleidooi om tot een andere citeertitel van de wet te komen, omdat ik eigenlijk hoop dat er nog voorstellen van het kabinet komen die het, meer dan deze voorstellen, verdienen om aangeduid te worden met de term "Cybersecuritywet". En wie wat bewaart, die heeft wat! Ik denk dat het amendement — iedereen zal er kennis van hebben genomen — voor zich spreekt. Ik wil daar verder maar niet te veel over uitweiden.

De laatste tijd komt er veel op ons af op het vlak van data en privacybescherming. Er is bedacht dat morgen de AVG in werking treedt. Die komt dus ook af op de bedrijven, die nu ook deze regelgeving op zich af zien komen. Kan de minister nog eens goed duiden welke belasting dit wetsvoorstel heeft voor Nederland, dat ook al druk doende is met de implementatie van de AVG?

Voorzitter. Dan het missen van de implementatietermijn. Er zijn volgens mij meer regels uit Europa die op ons afkomen, waarbij wij niet de snelsten zijn in het halen van de termijnen. Ik vind dat jammer. Soms is het, mede gelet op de kabinetswisseling, onvermijdelijk dat het zo is, denk ik. Maar ik meen dat er ook nog een richtlijn is over de bescherming van strafvorderlijke gegevens, het zusje van de AVG, die ook nog ligt te wachten en ook niet binnen de termijn komt. Wat zijn de consequenties daarvan? Moeten we denken aan een boete of komt Europa het hier dan overnemen? Kan de minister aangeven wat de consequenties zijn?

Dan de informatievoorziening naar burgers en bedrijven toe. Daar is ook al eerder door collega's op gewezen. Ik wil me daarbij aansluiten. In hoeverre zijn mensen, en vooral bedrijven, nu voorbereid dat ze hieronder vallen? Dat geldt met name ten aanzien van de DSP's, de digitaledienstverleners, want er moet nog bezien worden op welke manier zij hieronder vallen. De minister van Economische Zaken moet dat nog aanwijzen. Dreigt hier niet de situatie dat bedrijven te laat geïnformeerd worden?

Ook is het mogelijk om het ene jaar wel als DSP aangemerkt te worden en het jaar erna niet meer. "Dat ligt aan de aard van ondernemingen, die bedrijfsactiviteiten kunnen wijzigen", aldus de minister. Wel vraag ik me dan af waar de verantwoordelijkheid ligt. Is het aan de onderneming om scherp te zijn of ze het nog wel of niet meer is? Indien er een lijst komt van DSP's, moet men dan melden wanneer

de bedrijfsactiviteiten wijzigen? Waar ligt het initiatief van die karakterwijziging?

Dan over de nulmeting. Ten aanzien van het doen van een nulmeting in bepaalde sectoren vinden wij het antwoord van de minister enigszins teleurstellend. De minister beaamt dat het wellicht goed kan zijn om een inventarisatie te maken van de huidige situatie van veiligheid, maar daar lijkt het dan bij te blijven. Het is inderdaad aan de bevoegde autoriteit om het toezicht te organiseren, maar daar kan de minister toch wel aanbevelingen in doen, lijkt ons? Het lijkt mij echt een gemiste kans als dit niet wordt gedaan. Of heeft de minister al indicaties dat dit onderdeel zal worden van het toezicht?

Tot slot. Ik vraag mij af hoe wij als Kamer op de hoogte worden gehouden van de implementatie van deze wetgeving. Daar staat eigenlijk betrekkelijk weinig over in de wet en in de memorie van toelichting. Zou de minister bereid zijn om een rapportage naar de Kamer te sturen — ik denk dan aan een termijn van een jaar — over hoe het nu gaat met de invoering van deze wet? Hoeveel bedrijven vallen eronder? Hoe krijgt het toezicht nader vorm? Dat vraag ik mede ook gelet op het feit dat er aan de zijde van Economische Zaken in de tussentijd nog het nodige moet gebeuren.

Dank u wel.

De **voorzitter**:
Hartelijk dank. Dan geef ik het woord aan de heer Arno Rutte namens de VVD.

□

De heer **Arno Rutte** (VVD):
Voorzitter. Als je wat later in een debat aan de beurt bent dan is er soms ook al wat gras voor je voeten weggemaaid, zeker bij wetsbehandelingen waar Kamerleden het voor een heel groot deel met elkaar eens zijn. Laten we toch eens kijken waar ons dat brengt.

Ik ben het met de heer Alkaya eens dat digitale veiligheid net zo belangrijk is als fysieke veiligheid. Volgens mij zei mevrouw Buitenweg dat ook. We moeten constateren dat er eisen zijn ten aanzien van producten en diensten die bijdragen aan onze fysieke veiligheid. We stellen bijvoorbeeld eisen aan een dijk, over hoe die gebouwd moet worden om ervoor te zorgen dat we droge voeten houden. We stellen eisen aan auto's: zitten er airbags in en andere veiligheidssystemen in om zeker te weten dat we daar veilig in kunnen rijden, althans zo veel mogelijk? Dus is het ook logisch dat we eisen stellen aan cruciale digitale diensten. Het is ook goed dat dat nu op Europees niveau wordt geregeld, omdat in de digitale wereld alles met iedereen verbonden is. Als het speelveld binnen Europa gelijker is en we erop kunnen rekenen dat ook in andere lidstaten een voldoende veiligheidsniveau wordt betracht, kunnen we ook ons land digitaal een stuk veiliger houden. De dreigingen die op ons afkomen zijn door een aantal collega's net al heel duidelijk geschetst.

Het mag dan ook duidelijk zijn dat VVD voorstander is van het voorliggende wetsvoorstel. De heer Van Dam heeft het net al uitgelegd, met alle afkortingen van dien. We hebben te maken aanbieders van essentiële diensten, de AED's. Die vallen onder deze wet. We hebben ook de digitaledienstverleners, de DSP's. Het is een feest van de afkortingen. Laat ik een lang verhaal kort maken. Die AED's worden aangewezen door de overheid. Wie daaronder valt, is wel duidelijk. Dat weet je. Je krijgt een aanwijzing dat je moet voldoen aan deze wet. Zoals net een aantal collega's al aangaf, is dat bij die DSP's toch een stukje onduidelijker.

Ik zou wat inzicht willen geven in hoe onduidelijk dat is. Digitale serviceproviders of aanbieders van digitale diensten kunnen wel of niet onder die wet vallen. Er is een poging gedaan om daar wat uitleg aan te geven. Dan lees je dingen als dat een onlinemarktplaats of een digitale marktplaats eronder vallen. Dan wordt er een poging gedaan om een uitleg te geven: "Een onlinemarktplaats betreft een digitale dienst die producten of diensten van derden (ondernemers) aanbiedt en namens deze derde partij gedeeltelijk of in zijn geheel fases overneemt die deze derde partij zelf zou uitvoeren (bijvoorbeeld betaling, verzending, of aanbieden van een dienst/product)." Het valt natuurlijk enorm te prijzen dat de regering getracht heeft om een mooie omschrijving van wat het betreft in de wet te zetten. Die staat er ook voor andere termen die onder die digitale serviceproviders vallen, zoals onlinezoekmachines of cloudcomputerdiensten.

In de wetenschap dat de gemiddelde ondernemer doorgaans bezig is met ondernemen, geen wetten leest en als hij ze al leest misschien niet helemaal in het juridische jargon thuis is, kun je je voorstellen dat het in de praktijk onduidelijk is of je wel of niet onder die wet valt. Daar hebben andere partijen en ook wij vragen over gesteld. Dat antwoord dat in de schriftelijke beantwoording staat, stelt een beetje teleur. We kregen letterlijk het volgende antwoord. We kregen de toezegging dat het ministerie van Economische Zaken en Klimaat gaat kijken hoe tijdig naar dienstverleners gecommuniceerd kan worden over de wet, dat het het maken van een checklist overweegt en dat ook nog wordt onderzocht of er een lijst van digitale serviceproviders bijgehouden kan worden. "Onderzoeken", "overwegen" en "wellicht", maar over een halfjaar moeten ondernemingen wel voldoen aan deze wet. Dus dat is echt wat de VVD betreft toch wel erg mager, dat nadenken, onderzoeken en overwegen. Ik heb daarom ook een eenvoudige vraag aan de minister: hoe zorgt hij dat voor ondernemers op de implementatiedatum klip-en-klaar is of zij onder de definitie van de voorliggende wet vallen?

Dat met betrekking tot de wet. Enigszins bezijden daarvan wil ik vandaag graag een ander punt onder de aandacht brengen. Hoe belangrijk het ook is dat organisaties zelf hun digitale veiligheid goed organiseren, als er wat aan de hand is dan is het ook belangrijk dat er digitaal goed gerechercheerd wordt. We hebben een accuraat politiekorps nodig dat cybercriminelen in de kraag kan vatten, want anders houden we Nederland digitaal niet veilig. Ik heb in meerdere debatten aandacht gevraagd voor de kennis en de vaardigheden die daarvoor nodig zijn in het politiekorps en gevraagd of de politie toegang heeft tot dit soort mensen, of zij in staat is om die te werven. Dan zegt de minister steeds, en dat wil ik ook van hem geloven: de politie is een van de meest populaire werkgevers van Nederland en er wordt heftig geworven. Dat laatste is zeker waar. Je hoeft maar de radio aan te zetten en je hoort de spotjes waarin digitaal talent wordt geworven door de politie. Hartstikke goed, we hebben deze mensen ook heel hard nodig; een goede en terechte inspanning.

Ik heb de afgelopen maanden ook een rondgang gemaakt langs een groot aantal bedrijven waar iedere dag heel veel deskundigen werken aan cyberveiligheid. Onafhankelijk van elkaar melden deze bedrijven nu al enorme moeite te hebben om de benodigde mensen aan zich te kunnen binden. Het digitale talent, het cybertalent, is schaars en de concurrentie op arbeidsvoorwaarden is enorm. De kans dat de politie daar helemaal in mee kan gaan is eigenlijk nihil. We moeten niet willen dat de politie het soort bedragen gaat betalen dat in het bedrijfsleven wordt betaald; niet haalbaar. Tegelijker zien diezelfde organisaties het grote belang dat cyberkennis en -deskundigheid bij de politie voldoende aanwezig is.

In het Verenigd Koninkrijk zijn de afgelopen jaren forse stappen gezet met het zogeheten — ik ontkom niet aan de Engelse term; het gaat over het Verenigd Koninkrijk — Employer Supported Policing. De politie zoekt daar actief de samenwerking met het bedrijfsleven voor ondersteuning van werknemers uit die bedrijven om ingezet te worden als vrijwilliger bij de politie, vaak als platte pet — dat doen we in Nederland ook — maar steeds vaker ook als cyberdeskundige of als financieel rechercheur. Mensen uit de city, de krijtstreeppakken, werken ook als vrijwilliger om de financiële boeven aan te pakken. Voor cyberdeskundigheid geldt precies hetzelfde. Werkgevers betalen vaak de uren door, zodat de werknemer kan worden ingezet. Mede dankzij dat programma lukt het om de zeer schaarse cyberkennis en ook financiële kennis beschikbaar te maken voor de Britse politie in de vorm van politievrijwilligers, met steun van de werkgevers. Uit de gesprekken die ik heb gevoerd bleek dat ook Nederlandse werkgevers openstaan voor een dergelijke samenwerking. Ik vraag de minister om samen met de korpschef deze handschoen op te pakken en ook in Nederland tot een door werkgevers ondersteunde vrijwilligersinzet bij de politie te komen, te beginnen op het gebied van cybersecurity. Is hij daartoe bereid en, zo ja, op welke termijn wil hij dit dan gaan oppakken?

Voorzitter, dank.

De **voorzitter**:
Hartelijk dank. Dan geef ik het woord aan de heer Verhoeven namens D66.

□

De heer **Verhoeven** (D66):
Voorzitter. Ik ben blij dat we vandaag weer kunnen spreken over dit belangrijke onderwerp van cybersecurity, een onderwerp dat in belang toeneemt. Een paar jaar geleden was er relatief eigenlijk weinig aandacht voor, ook in deze Kamer. Nu hebben we regelmatig een debat. Ik denk dat dat een goede ontwikkeling is; noodzakelijk ook. Als de wereld verandert, moet de Tweede Kamer daar ook op inspringen en de onderwerpen die steeds nadrukkelijker op de mensen afkomen ook behandelen.

Vandaag praten we over de Cybersecuritywet, een naam die doet vermoeden dat het een zware, stevige, nieuwe wet is, maar dat is het natuurlijk niet. Het is gewoon een uitvoeringsimplementatiewet van de NIB-richtlijn van de Europese Unie, maar daarmee is het toch wel weer onderdeel van een bredere cybersecurity-agenda van dit kabinet, een agenda die ook goed gevuld is. Het kabinet erkent het enorme belang van cybersecurity en gaat daarmee ook concreet en daadkrachtig aan de slag. Zo wordt er 100 miljoen geïnvesteerd in cybersecurity, in onderzoek en het versterken van kennis en kunde op het gebied van ICT-voorzieningen bij de overheid. Mensen en bedrijven worden gestimuleerd om de basis op orde te hebben — met campagnes en digitale vaardigheden als onderdeel van het onderwijscurriculum. Er komt een Digital Trust Centre, het kabinet stimuleert het creëren van veilige apparaten en software door bijvoorbeeld verplichte eisen te stellen aan IoT-apparaten; de heer Alkaya had het er al over. IoT-apparaten ... Excuus, voorzitter. Dat zijn al die leuke apparaten die worden aangesloten op het internet, het internet der dingen. Er worden ook eisen gesteld op het gebied van software. Er wordt ook samenwerking tussen bedrijven en overheden gestimuleerd om snel te kunnen anticiperen en snel te kunnen inspelen op allerlei nieuwe ontwikkelingen. Dat is goed.

De wet die er nu is, past daar wel binnen. Deze wet regelt dat aanbieders van essentiële diensten en een aantal digitaledienstverleners adequate maatregelen moeten nemen om hun cybersecurity, hun cyberveiligheid dus, op orde te krijgen en dat ze incidenten moeten melden, zodat iedereen op een goede wijze van elkaar kan leren. Nederland was overigens al koploper op dit gebied, dus ook zonder die implementatiewet deden we het al goed en waren we al actief. Maar ik ben wel blij dat met deze richtlijn ook alle andere lidstaten in de Europese Unie aan dit onderwerp moeten werken en het beveiligingsniveau binnen de hele Europese Unie dus ook omhooggaat. Dat is een positieve ontwikkeling.

Ik heb nog een paar vragen en suggesties. Daarmee overlap ik wel wat met een aantal van de sprekers voor mij, maar dan zet ik hun woorden maar wat kracht bij door hun verhaal te herhalen en misschien te specificeren. Ik begin met de definitie van een DSP, een digitaledienstverlener. De heer Van Dam had het er ook al over. Welke bedrijven en organisaties zijn dat nu precies? Het kabinet heeft gezegd dat het ook bedrijven met meer dan 50 medewerkers kunnen zijn. Men gaat nog bezien op welke manier bedrijven zelf kunnen kijken of ze onder de definitie vallen, bijvoorbeeld via een vragenlijst. De vraag die ik aan de minister zou willen stellen, is wat de voortgang is op dat punt. Dat sluit ook een beetje aan bij de vraag van de heer Arno Rutte.

D66 probeert de lasten voor bedrijven zo laag mogelijk te houden, bijvoorbeeld door te zorgen dat het doen van meldingen gemakkelijk en laagdrempelig is. De minister heeft schriftelijk aan de Kamer een antwoord doen toekomen, waarin staat dat hij gaat onderzoeken of de meldingen kunnen worden gedaan via één handeling. Hoe staat het daarmee en op welke termijn krijgen we daar uitsluitsel over?

Dan een iets pikanter punt, voorzitter, al zeg ik het zelf. Dat laat ik ook even aan de minister. In de schriftelijke ronde heeft D66 gevraagd of ethische hackers erop kunnen vertrouwen dat onbekende kwetsbaarheden die zij vinden en die zij melden bij het NCC, niet ook door de politie, dan wel de diensten AIVD en MIVD gebruikt kunnen worden om te gaan hacken. De minister zei dat het soms inderdaad het geval zou kunnen zijn dat onbekende kwetsbaarheden worden doorgespeeld naar de AIVD. Althans, dat heb ik uit zijn antwoorden aan de Kamer gehaald. Klopt het dat informatie in die gevallen niet aan de maker van de software gemeld wordt? Die zou het gat natuurlijk gaan dichten en

als de maker het dicht, kunnen de diensten het niet meer gebruiken om ermee te hacken. Dat is steeds het dilemma op het gebied van de onbekende kwetsbaarheden, die ook wel zero-days genoemd worden. Hoe zit het daarmee? Hoe zit het met dat dilemma? Waar positioneert het kabinet zich als het gaat om het gebruik van de onbekende kwetsbaarheden die door ethische hackers gevonden worden om te melden, zodat het bedrijf ze kan sluiten, versus het belang van de dienst om ze open te houden? Het is een belangrijke kwestie, waar we toch uiteindelijk een keuze in moeten maken. Hoe vaak gebeurt dit? Ziet de minister de kwalijke gevolgen voor de onafhankelijke rol van het NCC? Ik zie het NCC als een onafhankelijke autoriteit en niet als een dubbelrol/doorgeefluik van onbekende kwetsbaarheden. Ik vind toch dat we daar echt scherp op moeten letten. Graag een antwoord van de minister hierop dat meer zekerheid biedt over deze keuzes.

Dan wil ik dit puntje afsluiten door te zeggen dat ethische hackers erop moeten kunnen vertrouwen dat de informatie die zij keurig hebben verkregen via de responsible disclosure, leidraden en alle dingen waar ze zich aan moeten houden, zorgvuldig behandeld wordt. Dus als ze met iets komen en iets vinden, moeten ze er zeker van kunnen zijn dat die informatie zorgvuldig behandeld wordt.

De **voorzitter**:
De heer Van Dam heeft een vraag voor u.

De heer **Van Dam** (CDA):
Ik hoor de heer Verhoeven over die zero-days praten. Volgens mij is dat onderwerp niet zozeer bij deze wet aan de orde, maar speelde het misschien meer een rol bij de Wet computercriminaliteit III. Dat hij het zo nadrukkelijk naar voren brengt, mag ik daaruit afleiden dat D66 een wellicht wat andere positie heeft ingenomen ten opzichte van dat onderwerp en dat ze dit met deze opmerking wil meegeven aan de minister?

De heer **Verhoeven** (D66):
Absoluut niet. Computercriminaliteit III, de wet waar de heer Van Dam het over heeft, gaat over de manier waarop de politie deze kwetsbaarheden gebruikt. Die wet is overigens in de Kamer behandeld. Dit is echter breder, want dit gaat over de AIVD en de MIVD. Die worden niet door de Wet computercriminaliteit III aangestuurd, om het zo maar te zeggen. Die worden aangestuurd door een andere wet, die wij overigens allen in deze Kamer aan de orde hebben gehad, de Wiv. Een heel interessante wet waarover u meer zou moeten weten, voorzitter. Dat even terzijde.

Nee, dit is niet om een inleiding te geven op een standpunt van D66. Dit is een vraag aan de minister over een dilemma dat los van deze twee wetten staat. Het is dus van belang om er een heldere aanpak voor te krijgen. Dat vraag ik dus aan de minister.

De **voorzitter**:
De heer Van Dam, ten slotte.

De heer **Van Dam** (CDA):
Kan de heer Verhoeven mij misschien nog even helpen? Welke rol vervullen die ethische hackers dan in het kader van deze wet ten aanzien van de meldplicht of überhaupt van dit soort bedrijven, want daar hebben we het vooral over in het kader van deze wet? Dat snap ik niet helemaal.

De heer **Verhoeven** (D66):
De verhouding tot deze wet is de volgende. Ethische hackers melden bepaalde kwetsbaarheden, bekend dan wel onbekend, aan bedrijven die daar vervolgens mee aan de slag moeten. Dat valt zeker binnen de strekking van deze wet, want die gaat ook over het melden van kwetsbaarheden. Als dat gebeurt, wordt de vondst van die ethische hackers, de onbekende kwetsbaarheid die zij hebben gevonden, zonder dat zij het zelf weten doorgespeeld aan de politie of de inlichtingen- of veiligheidsdiensten, terwijl dat niet de reden was waarom zij die aan het NCSC gemeld hebben. Op die ontwikkeling wil ik graag grip hebben. Ik wil dus graag van de minister weten hoe dat in z'n werk gaat. Ik zie dat de heer Van Dam nu ook wakker is geworden en dat hij ook ziet dat wij als Kamer wel degelijk heel goed op dit punt moeten letten. Ik ben dus blij dat hij die vraag nog even kon stellen.

Ik wil nog even naar de zorgsector, als dat mag, voorzitter. Bij de WannaCry-aanval — dat was de naam van de ransomwareaanval die zich deze zomer heeft voorgedaan en die natuurlijk redelijk zorgelijk is uitgepakt — zijn meerdere ziekenhuizen in Europa getroffen. We hebben daar met de vorige bewindspersonen ook over gesproken. Als gevolg van die aanval konden sommige mensen geen behandeling krijgen. In het Verenigd Koninkrijk konden sommige mensen zelfs geen chemokuur krijgen. De zorg lijkt me dus bij uitstek wel een vitale sector, letterlijk eigenlijk. De gegevens die zorgaanbieders hebben, zijn ook gevoelig. De systemen die ze gebruiken, bijvoorbeeld scanapparaten of medische apparatuur, zijn vaak van cruciaal belang voor patiënten. Daar komt dan nog eens de complexiteit bij dat die apparaten niet altijd snel vervangen of geüpdatet kunnen worden en dat dan dus extra risico oplevert. Daar hebben we het hier in de Kamer ook weleens over gehad. Maar in de zorgsector zijn geen AED's, aanbieders van essentiële diensten, aangewezen. Dat is wat D66 betreft toch merkwaardig. Wij willen dus graag van de minister weten waarom dat niet het geval is. Waarom heeft hij daar niet voor gekozen?

Gelukkig is er dit jaar al wel een Zorg-CERT, een cybersecurity emergency response team voor de zorg opgericht. Die organisatie moet snel kunnen inspelen op cyberaanvallen. Daar werken een aantal specialisten om zorginstellingen te helpen en wordt informatie gedeeld. Hoe staat het met de ontwikkeling van deze speciale CERT voor dat speciale team in de zorgsector? Zijn alle ziekenhuizen inmiddels aangesloten? Is de minister van mening dat er voldoende aandacht is voor cyberveiligheid in de zorg?

De **voorzitter**:
Hartelijk dank. Daarmee is een einde gekomen aan de eerste termijn van de Kamer. Heeft de minister behoefte aan een schorsing? Dat is het geval.

De vergadering wordt van 19.31 uur tot 19.45 uur geschorst.

De **voorzitter**:
Ik geef het woord aan de minister.

Minister **Grapperhaus**:
Voorzitter. Ik zal het wetsvoorstel niet te vaak bij naam noemen, omdat er een amendement is ingediend over de benaming. Dit wetsvoorstel bouwt verder op het fundament dat wij gelegd hebben met de Wet gegevensverwerking en meldplicht cybersecurity. Die wet regelt de taken van het Nationaal Cyber Security Centrum, het regime voor het verwerken van gegevens en een meldplicht voor ernstige incidenten bij hetzelfde Nationaal Cyber Security Centrum. Onderdelen komen terug in het wetsvoorstel. Los daarvan zitten er alleen maar bepalingen in ter implementatie van de zogenaamde NIB-richtlijn van de Europese Unie over de beveiliging van netwerk- en informatiesystemen, zoals de bepalingen die regelen dat aanbieders van essentiële diensten hun ICT passend moeten beveiligen en daarop ook toezicht moeten houden. Hetzelfde geldt voor aanbieders van online marktplaatsen, online zoekmachines en clouddiensten. Wij hebben ervoor gekozen om in het wetsvoorstel de rollen van hulpverlener (het al genoemde CSIRT) en toezichthouder (de bevoegde autoriteit) gescheiden te houden en om toezicht en sancties onder te brengen bij de bestaande sectorale toezichthouders, zoals De Nederlandsche Bank en het Agentschap Telecom. Ik zal daar straks nog wat uitvoeriger op ingaan, naar aanleiding van de vragen van het lid Buitenweg.

Ik kom tot de beantwoording van de gestelde vragen. Allereerst ga ik in op de vragen over de reikwijdte van het wetsvoorstel. In dit wetsvoorstel worden geen minimale eisen voor alle apparaten gesteld. Het is immers vast kabinetsbeleid om bij de implementatie van Europese wetgeving geen andere onderwerpen mee te nemen. Een van de redenen voor dat beleid is dat de implementatie vertraagd kan worden door het in de discussie meenemen van andere onderwerpen. De NIB-richtlijn gaat niet over eisen en apparaten, maar over het beveiligen van ICT-systemen die cruciaal zijn voor het goed functioneren van de samenleving.

Kunnen apparaten worden verplicht om apparaten te beveiligen tegen hacks en dergelijke? Waarom staat dat niet in het wetsvoorstel? De ontwikkelaars van software en hardware en de fabrikanten zijn uitgesloten van de NIB-richtlijn. Recent heeft mijn collega, de staatssecretaris van Economische Zaken, de Roadmap Digitaal Veilige Hard- en Software aan de Kamer gezonden. Die komt uitvoerig aan de orde in de Cybersecurity Agenda; laat dat duidelijk zijn. Daar zit een duidelijk verband in het beleid.

Met de genoemde roadmap kan de digitale veiligheid van projecten worden verbeterd. Onder meer wordt gekeken naar de wettelijke eisen om onveilige producten van de markt te weren, alsmede naar het stimuleren van standaarden en certificering bij de ontwikkeling van veilige producten. Bij de verdere uitwerking van de roadmap zullen ook eventuele verplichtingen van fabrikanten verder worden bekeken en geformuleerd.

De **voorzitter**:
De heer Alkaya heeft een vraag.

De heer **Alkaya** (SP):
Met alle respect, maar dat vind ik een vrij dogmatische manier om ernaar te kijken. Het is staand beleid om per definitie altijd tegen nationale koppen te zijn, terwijl hier sprake is van minimumharmonisatie en er een motie ligt die past bij het kabinetsbeleid om dat soort wettelijke maatregelen voor apparaten te onderzoeken. Dat zou volgens mij kunnen door de reikwijdte van de wet op te rekken en daar niet alleen organisaties, maar ook fabrikanten van dit soort apparaten onder te laten vallen. Dat lijkt mij een vrij efficiënte en meer effectieve manier van werken dan het inzetten van een heel ander traject.

Minister **Grapperhaus**:
Ik vrees toch dat ik hier een iets andere kant op denk. Als we het hebben over het efficiënt tot stand brengen van deze wetgeving en overige regelgeving, lijkt het mij goed om deze implementatiewetgeving nu voor te leggen en tegelijkertijd de roadmap uit te leggen, samen met de bedrijven. Dat doet de staatssecretaris van Economische Zaken. Vervolgens kunnen wij bekijken — daar moeten wij het nog over hebben — hoe ver de verplichtingen van fabrikanten zich precies zouden moeten uitstrekken. Als wij dat debat nu met elkaar gaan voeren, zijn wij echt een aantal maanden verder. Dat is niet een dogmatische keuze in de trant van: zo doen wij het nu eenmaal altijd. De reden dat ik ernaar verwees dat dit vast kabinetsbeleid is, is omdat dat nou eenmaal de efficiënte manier is om met implementatiewetgeving door te komen. Ik heb vrij uitvoerig geschetst waar mijn collega Mona Keijzer mee aan de slag is. Daarmee komt zij bij de Kamer terug, dat weet u. Daar ligt ook die door het lid gewenste efficiency en voortgang op dit punt in besloten.

Mevrouw **Buitenweg** (GroenLinks):
Ik kan de redenering van de minister in dit geval wel volgen, maar ik wil alleen afdingen op het feit dat dit kabinetsbeleid is. Naar ik meen gaan we binnenkort spreken over PNR, de passagiersgegevens, en daar zet het kabinet er toch een flinke kop op. Ik kan mij voorstellen dat u in dit geval vindt dat er reden is om een aantal zaken uit elkaar te halen, maar om te zeggen dat dit altijd vast kabinetsbeleid is ... Dat is toch vooral een beetje wanneer het u uitkomt. Dat mag, maar laten we dan niet zeggen dat dit de standaard is, want dat moet de standaard zijn.

Minister **Grapperhaus**:
Voor zover u verwijst naar PNR moet ik dat verwijt dat ik doe zoals het mij uitkomt, toch naast me neerleggen, maar ik wil dat zo hoffelijk mogelijk doen. We komen nog over PNR te spreken. Op enig moment is door de Raad van Ministers in Europa een ook aan uw Kamer destijds gemelde nadere afspraak gemaakt en daarover wordt nu gesproken. Dat is toch iets anders, juridisch gezien, dan een zuiver nationale kop.

U noemt dit voorbeeld, maar voor het overige is er het gebruik, niet als een soort oud-Hollandse traditie, maar omdat we moeten zorgen dat we efficiënt Europese regelgeving implementeren, dat we het in beginsel houden bij wat in de richtlijn staat. Hoezeer ik ook sympathiseer met de door de heer Alkaya naar voren gebrachte punten, laat dat duidelijk zijn, dat zou een te grote extra belasting voor

het schip van deze implementatiewet worden. Nogmaals, ik heb gezegd dat het kabinet daar wel actief mee bezig is via de staatssecretaris EZ.

De **voorzitter**:
Mevrouw Buitenweg, ten slotte.

Mevrouw **Buitenweg** (GroenLinks):
Inderdaad, we komen nog over PNR te spreken. Het gaat nu over implementatie van richtlijnen. In de richtlijn over PNR staat iets wat veel minimaler is dan wat het kabinet heeft afgesproken met zijn collega's. Dat laatste staat nergens in een wet, dus ik handhaaf de stelling dat het nu is zoals het de minister uitkomt. Ik kan mij ook goed voorstellen dat hij hiervoor kiest. Ik hoop hem bij PNR ertoe over te halen om ook dan voor een minimale implementatie te kiezen.

Minister **Grapperhaus**:
Ja, ik vind het heel goed dat we hier en daar ook al een blik vooruitwerpen op wat nog komt, maar ik blijf herhalen dat het door het lid Buitenweg gemaakte verwijt naar mijn oordeel echt niet terecht is.

Zal ik doorgaan, voorzitter?

De **voorzitter**:
Ja, natuurlijk.

Minister **Grapperhaus**:
Dan kwam ik op een aantal vragen over digitaledienstverleners. Ik zal deze Nederlandse term voor de Engelstalige afkorting DSP blijven hanteren. Hoe worden die digitaledienstverleners aangewezen? Ik heb er al op gewezen, zoals de heer Rutte ook overwoog, dat de staatssecretaris van Economische Zaken beziet hoe tijdig kan worden gecommuniceerd. Ik begrijp heel goed dat het lid Rutte zegt dat hij toch graag wil dat dit iets verder gaat. Ik zeg toe dat ik met de staatssecretaris hierover zal spreken, bij haar het belang van dit punt zal benadrukken en met haar zal bezien in hoeverre we die tijdige communicatie zo scherp en actief mogelijk kunnen maken.

De **voorzitter**:
De heer Rutte heeft hier nog een vraag over.

De heer **Arno Rutte** (VVD):
Ik heb niet heel veel vragen gesteld, maar deze wel. Het punt is dat al eerder in de schriftelijke ronde gevraagd is om concreet te maken wat er gaat gebeuren. Toen kwam als antwoord: wij denken aan, en er stonden een aantal opties; we zouden zus, we zouden zo et cetera. Nu zegt de minister dat hij zich er hard voor gaat maken en in een goed gesprek met de staatssecretaris gaat vertellen dat wij dit heel belangrijk vinden, om het een beetje samen te vatten. Kan hij nou waarborgen dat, als die wet straks is geïmplementeerd — dat is in principe over ongeveer iets meer dan een halfjaar — er geen onduidelijkheid is, dat iemand die onder die omschrijving valt, weet dat dit zo is, dat kan weten en niet hoeft te twijfelen omdat de communicatie op orde is?

Minister **Grapperhaus**:
Mag ik dan toch via u, voorzitter, voor de heer Rutte meteen even een vraag beantwoorden waarin ik hierop terugkom? Dat is namelijk de vraag: welke bedrijven zijn nu digitaledienstverleners? Digitaledienstverleners zijn de bedrijven die, uiteraard, in de digitaledienstverlening werkzaam zijn en waar 50 of meer personen werkzaam zijn of die een jaaromzet hebben van 10 miljoen of meer. Zij vallen onder de richtlijn. Ik herhaal nu een beetje wat ik heb gezegd. De staatssecretaris bekijkt hoe je dat kunt nagaan aan de hand van een checklist. Daarin zit een toetssteen: in hoeverre moet een onderneming die een digitale dienst aanbiedt, een online marktplaats bijvoorbeeld, als een digitaledienstverlener worden aangemerkt? Uiteraard moet ook in die communicatie zitten bij wie men terechtkan om dat te testen.

Hierbij speelt natuurlijk het volgende algemene punt. Er komt nieuwe wetgeving waarin gedefinieerd wordt welke partijen een verplichting hebben, de AED's of, in dit geval, de digitaledienstverleners. Daar wordt een definitie van gegeven. Terecht wijst de heer Rutte erop dat niet altijd iedere ondernemer precies even goed … Dat zou wel moeten, want eenieder wordt geacht de wet te kennen. Maar goed, dat schiet er weleens bij in. Vandaar dat we zo'n communicatiecampagne bekijken. Mijn toezegging ging iets verder dan dat ik mij hard zal maken voor een gesprek dat ik ga voeren met de staatssecretaris. Mijn toezegging is: ik ga met de staatssecretaris in gesprek om te kijken hoe we die communicatie en bewustwording bij bedrijven die volgens deze wet mogelijk digitaledienstverlener zijn, zo inrichten dat die bedrijven dat ook echt even goed bij elkaar checken.

In het verlengde daarvan is natuurlijk de vraag opgeworpen hoe het zou moeten zijn als zo'n bedrijf op enig moment een andere activiteit onderneemt. Nou ja, op het moment dat een bedrijf ervoor kiest om zijn bedrijfsvoering te wijzigen, bijvoorbeeld door activiteiten af te stoten en daardoor onder de omzetgrens te vallen, of juist door te acquireren en naar boven te vallen … Het is op een gegeven moment natuurlijk wel de verantwoordelijkheid voor een bedrijf om zelf te controleren of men nog wel of niet meer onder deze wet valt. Naarmate men in de professionele wereld meer met die wet bekend is, mag men natuurlijk ook worden geacht daar meer bewustzijn van te hebben. Ik hoop dat ik daarmee geantwoord heb.

De **voorzitter**:
Ik denk nog niet voldoende.

Minister **Grapperhaus**:
O, nou ja.

De heer **Arno Rutte** (VVD):
De minister legt het heel uitvoerig uit. Dat valt te prijzen en dat is ook goed. De dingen worden wat meer duidelijk, maar toch. De vraag is niet alleen of je door een bepaalde omvang onder de wet valt. Nee, de vraag is bijvoorbeeld ook: heb

ik een digitale marktplaats, ja of nee? Er staan in de wet wel allerlei dingen omschreven. In het ene geval wel, in het andere geval niet. Soms een beetje, soms niet helemaal. Cloud computing diensten: idem dito. Ik kan mij voorstellen dat ondernemers daaraan twijfelen. Dus aan de ene kant hoor ik: we gaan de communicatie richting ondernemers in zijn algemeenheid op orde brengen. Nou, dat wil ik geloven. Maar kunnen ondernemers die twijfelen nu ook ergens terecht, zo van "ik doe dit, dit is mijn onderneming en ik wilde even zeker weten of ik aan de regels voldoe"?

Minister **Grapperhaus**:
Ik zei het net, maar ik wil dat toch nog echt even benadrukken. Natuurlijk moeten wij bij een soort mogelijkheid van een toetsingslijst ook de mogelijkheid betrekken — maar dat zal echt bij EZK liggen — om te kijken waar men terecht kan met dit soort vragen. In mijn jeugd heette dat Postbus 51, maar er moet inderdaad ook een soort loket zijn waar men met vragen terechtkan.

Voorzitter. Dan kom ik op de vraag hoe het CSIRT voor digitaledienstverleners wordt aangewezen, nu dat niet in de wet zelf gebeurt. Na de nota van wijziging bepaalt het wetsvoorstel dat het CSIRT voor digitaledienstverleners wordt aangewezen bij klein Koninklijk Besluit. Dat kan heel snel. Als zodanig zal een DTC worden aangewezen, een Digital Trust Center. De heer Verhoeven refereerde daar al aan. Dat is nu in oprichting en wordt een onderdeel van het ministerie van Economische Zaken.

Dan had ik nog wat vragen van de heer Van Dam over de deadline van de implementatie. Hij vroeg: wat zijn de consequenties als we de deadline niet halen? De NIB-richtlijn kent twee implementatietermijnen. De eerste is verstreken op 9 mei. Die datum geldt alleen voor het centrale contactpunt, voor digitaledienstverleners en voor de mogelijkheid van vrijwillige melding van incidenten. De tweede termijn verstrijkt op 9 november en we verwachten die te gaan halen. Nederland is niet de enige lidstaat die te laat is; wij zitten in de middenmoot. Op zichzelf is de Europese Commissie nu bevoegd om tegen Nederland een ingebrekestellingsprocedure te beginnen voor het niet halen van de datum van 9 mei, maar zo'n procedure neemt veel tijd in beslag, met veel tussenstappen. Ik heb goede hoop dat Nederland op tijd het been gaat bijtrekken, om nog een sportterm te gebruiken.

Dan is er gevraagd naar Kaspersky. Mevrouw Buitenweg heeft gevraagd hoe zo'n besluit tot stand komt. Zijn er bewijzen voor? Zijn er nog andere leveranciers die problemen kunnen veroorzaken? Welnu, ik wil vooropstellen dat we vanavond spreken over de Cybersecuritywet. Ik wil dus ook niet te veel ingaan op de Kasperskycasus. Ik heb uw Kamer daar een brief over gestuurd en het lijkt me zaak dat we die brief eventueel in een debat behandelen, want dit gaat ook veel meer over buitenlandse inmenging. Ik wil wel aangeven hoe we tot het besluit zijn gekomen en wat dat betekent. Een drietal factoren heeft voor dit besluit gezorgd. De eerste was dat de antivirussoftware van Kaspersky heel diep in de systemen zit. Dat heeft een risico in zich, want als er op enig moment vanuit een verplichte instructie van de Russische overheid mee gemanipuleerd wordt, kan dat heel diep in die systemen ernstige gevolgen hebben. De tweede is Russische regelgeving die bedrijven verplicht om mee te werken. De derde is dat de Russische overheid een offensief cyberprogramma heeft gericht op Nederland en Nederlandse belangen. Ik heb vorige week uiteengezet dat dat laatste is gebaseerd op inlichtingen van onze diensten. Zoals gezegd moeten we over de vraag hoe dit zich zou moeten verhouden tot bijvoorbeeld andere bedrijven of misschien zelfs wel andere landen, het debat aangaan naar aanleiding van de Kasperskybrief.

De **voorzitter**:
Ik constateer dat dit onderwerp maar zeer zijdelings aan de orde is, maar omdat de minister besloten heeft om er toch op in te gaan, wil ik mevrouw Buitenweg de mogelijkheid geven om hier één vraag over te stellen.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel. Ik stel die vraag naar aanleiding van het feit dat een collega van de minister het nadrukkelijk naar vanavond en naar de minister verwees afgelopen middag. Vandaar dus dat ik het nu aan de kaak stel. Mag ik de minister vragen om een aanvullende brief, waarin hij beschrijft wat de eisen op dit gebied zijn en voor wie ze gelden? Want het raakt wel heel veel bedrijven, die ook in aanbestedingsprocedures zitten. Mogen zij bijvoorbeeld nog wel deze software gebruiken of niet? Hoe zit het nu precies in elkaar? Welke eisen stellen we om te zorgen voor voldoende veiligheid? Ik denk dat het in het belang van bedrijven is dat zij weten waar zij aan toe zijn en ik denk dat die duidelijkheid nu nog niet gegeven wordt door de overheid.

Minister **Grapperhaus**:
Ik vind het wat lastig om nu al over de vorige brief heen een brief toe te zeggen als we over die vorige brief nog niet echt met elkaar gedebatteerd hebben, mede omdat dit een onderwerp is dat maar een heel klein beetje aan dit debat raakt, wat de voorzitter onderschrijft, begrijp ik. Dat zeg ik niet om mevrouw Buitenweg weg te sturen of iets dergelijks, wat trouwens ook helemaal niet in mijn vermogen zou liggen. Ik wil alleen maar aangeven dat ik haar gevoelen deel dat het goed is dat we met elkaar spreken over deze problematiek, maar dat ik zou willen voorstellen om dat eerst te doen aan de hand van de aan uw Kamer geschreven brief. Vervolgens is het, aan de hand van wat er uit dat debat voortkomt, misschien nuttig om een aantal dingen nog eens nader uit te werken voor uw Kamer. De centrale term — en daar wil ik het verder bij laten — in dit soort zaken is natuurlijk "nationale veiligheid".

De heer Verhoeven heeft een vraag gesteld over de kwestie van onbekende kwetsbaarheden. Als onbekende kwetsbaarheden bij het NCSC worden gemeld, worden die dan door de dienst of de politie gebruikt? Welnu, ik benadruk dat bij het NCSC het verhelpen van een onbekende kwetsbaarheid vooropstaat.

De **voorzitter**:
Ook dit onderwerp is maar zeer zijdelings aan de orde, maar ik wil de heer Verhoeven toch graag de mogelijkheid geven om één vraag te stellen.

De heer **Verhoeven** (D66):
Het is niet zijdelings aan de orde, het is onderdeel van de schriftelijke beantwoording van de minister over deze wet. Het is absoluut niet zijdelings. Ik zal het wel kort houden, voorzitter, maar dat spreekt eigenlijk voor zich. Het staat voorop, ja dat weet ik, maar ik vroeg natuurlijk of de minister duidelijkheid kan bieden dan wel kan uitsluiten dat dat gebeurt.

Minister **Grapperhaus**:
Met te zeggen "het staat voorop" bied ik duidelijkheid. Ik denk dat de heer Verhoeven niet verbaasd kan zijn als ik zeg dat ik daarover geen uitsluiting ga geven. Het kan zijn dat er een situatie is waar het belang van de nationale veiligheid speelt, waar het NCSC mogelijkerwijs wel degelijk de diensten van informatie moet voorzien over een onbekende kwetsbaarheid. Dat is niet uit te sluiten. Door te zeggen, zoals ik begonnen ben, dat het verhelpen van de onbekende kwetsbaarheid vooropstaat, wil ik alleen heel duidelijk aangeven dat dat het uitgangspunt is. Dat is de regel, waarop heel soms een uitzondering mogelijk is, in het kader van die nationale veiligheid.

De **voorzitter**:
De heer Verhoeven tot slot.

De heer **Verhoeven** (D66):
Dit is absoluut duidelijker, en dank daarvoor. Sommige dingen sluit het kabinet wel uit, sommige dingen sluit het kabinet niet uit. Dit sluit het kabinet niet uit. Dat is helder. De minister laat ook weten waarom. Ik kom er in mijn tweede termijn nog wel even kort op terug. Ik wil de minister wel vragen hoe er, mocht het dan in die uitzonderlijke situatie gebeuren, wordt omgegaan met de ethische hacker in kwestie die de onbekende kwetsbaarheid heeft aangereikt bij het Nationaal Cyber Security Centrum.

Minister **Grapperhaus**:
Ik zit even te denken. Daar wil ik op mijn beurt ook even in tweede termijn iets over zeggen, als u dat goed vindt.

De **voorzitter**:
Dan komt de minister daar in tweede termijn op terug.

Minister **Grapperhaus**:
Ja, ik begrijp dat punt wel, maar daarover moeten wij elkaar even goed toespreken in de tweede termijn.

Mevrouw Buitenweg heeft gevraagd of drie meldingen bij een incident niet te veel van het goede zijn en of er niet één loket zou moeten zijn. Het klopt dat het bij bepaalde incidenten zo kan zijn dat een aanbieder dat bij drie verschillende instanties moet melden. Ik noem ze maar even. Bij het CSIRT, bij de bevoegde autoriteit en dan eventueel ook nog eens de AP, de Autoriteit Persoonsgegevens, als er persoonsgegevens in het geding zijn. Die drie instanties hebben nadrukkelijk onderscheiden taken die maken dat ze alle zo direct mogelijk melding moeten ontvangen van een ernstig incident. Het NCSC als het in dat geval het CSIRT is — al die afkortingen voor het publiek elke keer — om hulp te verlenen. Bij de bevoegde autoriteit moet je het melden vanwege de toezichtfunctie en bij de Autoriteit Persoonsgegevens voor die specifieke toezichthoudende taken op de persoonsgegevens.

Wij streven ernaar — mevrouw Buitenweg wees daar terecht op — om de lasten als gevolg van die meldplichten technisch zo in te richten dat het melden bij die instanties uiteindelijk maar één handeling zou vergen, want dat scheelt een enorm stuk voor iedereen. Vakdepartementen, toezichthouders en NCSC zijn daarover momenteel druk in overleg en zullen later dit jaar, als het goed is, tot een besluit komen. Daarnaast zal met de Autoriteit Persoonsgegevens worden bezien of op enig moment met zo weinig mogelijk extra lasten aan die meldplicht kan worden voldaan.

De heer Van Dam heeft een vraag gesteld over de administratieve lasten voor bedrijven als gevolg van de dubbele meldplicht. Naar verwachting zal de meldplicht in het wetsvoorstel dat nu nog "Cybersecuritywet" heet, niet leiden tot een groot aantal meldingen voor aanbieders van essentiële diensten en digitaledienstverleners — AED's en DDV's, zoals ik ze dan maar even noem — omdat alleen ernstige incidenten gemeld moeten worden. De inschatting, mede op basis van de in de huidige wet gemaakte inschattingen, is als volgt. Men verwacht per jaar bij de aanbieders van essentiële diensten maximaal tien tot twintig meldplichtige incidenten en bij digitaledienstverleners maximaal vijftien meldplichtige incidenten. De dubbele melding en de extra vervolghandelingen per incident zullen naar schatting gemiddeld 300 minuten betreffen. Voor aanbieders van essentiële diensten gaat het dan per incident om 40 minuten extra ten opzichte van de meldplicht bij het NCSC waaraan nu al moet worden voldaan. Voor de digitaledienstverleners, die nu nog niet onder de meldplicht vallen, bedragen nieuwe administratieve lasten per incident dus 300 minuten. Laten we even heel goed benadrukken dat we het dan wel over ernstige incidenten hebben. 300 minuten gedeeld door 60, dat is vijf uur. Dat is best veel tijd, maar een ernstig incident verdient wel die aandacht.

Zoals ik al heb gezegd in antwoord op een vraag van het lid Buitenweg, er wordt naar gestreefd om de meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt om zo de administratieve lasten te reduceren.

De **voorzitter**:
Mevrouw Buitenweg heeft hier toch nog een vraag over.

Mevrouw **Buitenweg** (GroenLinks):
U gaf ook een aantal uren aan. Wat is nu het aantal uren waarbinnen gemeld moet worden? Hier staat "zo snel mogelijk" terwijl er bijvoorbeeld bij de AVG een meldplicht van 72 uur is. Kan dat niet vergelijkbaar zijn?

Minister **Grapperhaus**:
Ik had ernaar verwezen dat nieuwe administratieve lasten per incident 300 minuten belopen. Dat is vijf uur. Sorry, ik dacht dat ik dat duidelijk heb gezegd, maar het kan zijn dat dat niet het geval was.

Mevrouw **Buitenweg** (GroenLinks):
Kan ik dan sowieso de vraag stellen over de uren, de meldplicht en de tijd waarbinnen een melding moet zijn gedaan? Bij de AVG is dat 72 uur. Hier staat "zo snel mogelijk". Is het mogelijk om daar een gezamenlijke lijn in te trekken?

Minister **Grapperhaus**:
U wilt daar een lijn in trekken? Dan moet ik even nadenken, want er zijn wel wat wezenlijke verschillen. Dat komt nog aan de orde bij een aantal vragen over de AVG, die ik nog ga beantwoorden. Die pak ik er dan toch maar eventjes bij. Voorzitter, ik hoop dat u het goedvindt dat ik even naar die vraag spring. Mevrouw Buitenweg vroeg of de implementatie vergelijkbaar is met die van de AVG, de Algemene Verordening Gegevensbescherming. Dan zeg ik: nee, het wetsvoorstel is nauwelijks vergelijkbaar met de AVG. Die gaat over de bescherming van persoonsgegevens terwijl de NIB-richtlijn de lidstaten opdraagt om werk te maken van de beveiliging van ICT, die cruciaal is voor het goed functioneren van de samenleving. Dat zijn toch echt twee behoorlijk uit elkaar liggende activiteiten. Mevrouw Buitenweg vroeg of we dit nu ook zo snel mogelijk zouden kunnen invullen langs de lijn van 72 uur. Ik wil er even over nadenken hoe we dat zouden kunnen doen. Daar kom ik in tweede termijn nog even op terug.

De heer Verhoeven vroeg waarom er binnen de zorgsector geen aanbieders van essentiële diensten worden toegewezen. En hoe staat het met de oprichting van het Zorg-CERT? Om te beginnen, er zijn en worden uiteraard allerlei maatregelen genomen om de ICT in de zorg adequaat te beveiligen. Maar zorg is geen deel van de vitale infrastructuur, zoals gedefinieerd in de regelgeving. Er is grote diversiteit in aanbieders, en er is een mogelijkheid tot onderlinge vervangbaarheid in de zorgsector. Daarom worden er in die sector geen vitale aanbieders c.q. aanbieders van essentiële diensten aangewezen.

Dan het Zorg-CERT. Er is een sectorale CERT opgericht voor de gehele zorgsector. Dat is specifiek belast met monitoring, preventie en herstel van ICT-incidenten in de zorg. Voorts heeft het ministerie van VWS samen met de grote koepels in de sector een actieplan opgezet voor de verhoging van de veiligheid van patiëntgegevens. De minister voor Medische Zorg zal u daar periodiek over informeren.

De **voorzitter**:
De heer Alkaya heeft op dit punt een vraag voor u.

De heer **Alkaya** (SP):
Het is niet mijn punt, maar het is wel een belangrijk punt. Begrijp ik het goed dat er op dit moment voor toekomstige ontwikkelingen in de zorg, met allerlei patiëntendata, waar we allemaal kritische vragen over hebben, geen verplichting in de wet staat om dat soort diensten goed te beveiligen?

Minister **Grapperhaus**:
We moeten het even goed zien. Ik heb uitgelegd dat de zorg geen deel uitmaakt van de vitale infrastructuur, zoals die onder de richtlijn is komen te vallen. Ik heb ook uitgelegd waarom dat zo is. Ik wil dat niet nog een keer herhalen, als u mij dat niet euvel duidt. Dat neemt niet weg dat er wel andere maatregelen zijn genomen om de ICT in de zorg adequaat te beveiligen; dat heb ik ook onderstreept. Maar daar gaat het vandaag niet zozeer over. Vandaag gaat het over de toelichting op deze wetgeving.

De **voorzitter**:
De heer Alkaya, ten slotte.

De heer **Alkaya** (SP):
Uiteraard. Ik wil niet met de minister in een definitiekwestie komen over wat een vitale dienst is en wat niet. Volgens mij gaat het vandaag om de vraag: welke organisaties zouden volgens ons straks onder deze wet moeten vallen, of in ieder geval onder de wettelijke verplichting moeten vallen om hun systemen degelijk te beveiligen? Ik lees in de memorie van toelichting dat er niet is voorzien om zorginstellingen onder deze wet te laten vallen. D66 heeft daar terecht aandacht voor gevraagd. Dit staat los van de vraag wat een vitale dienst is, want het staat de minister vrij om alsnog te zeggen: voor deze sectoren vind ik het alsnog belangrijk dat zij systemen goed beveiligen, want zij werken met patiëntendata. Hoe kan de minister dan ... Of laat ik het anders vragen. Sluit de minister uit dat in de toekomst zorginstellingen altijd niet als AED zullen worden aangewezen? Of kunnen die volgens deze wet alsnog als AED, dus als vitale dienst, worden aangewezen, zodat zij ook hun beveiliging op orde moeten krijgen?

Minister **Grapperhaus**:
Ik wil daar meteen over zeggen dat ik niet iets per definitie ga uitsluiten. Er kan een toekomstige ontwikkeling in de zorgsector zijn die tot een zodanige situatie leidt dat zorginstellingen wel degelijk alsnog in deze wet zouden worden opgenomen. Dat kan ik niet uitsluiten. De toekomst is een beetje een glazen bol. Maar ik wil terug naar wat ik net uiteen heb gezet. Het is een optelsom van twee elementen. Het ene element — daar ben ik ook mee begonnen — is: let wel, er zijn allerlei andere maatregelen genomen om die beveiliging in de zorg adequaat te regelen. Het tweede element is dat deze regelgeving nou eenmaal een omschrijving geeft van wat vitale infrastructuur is, dus: wat moet volgens deze richtlijn nu precies onder deze regels vallen? Onder die definitie valt de zorgsector op dit moment niet. Die twee elementen tezamen vormen de uitleg van waarom zorginstellingen niet als aanbieders van essentiële diensten zijn aangewezen. Let u vooral op het eerste element. Daar moeten we het nu vandaag niet over hebben, maar in de zorg zijn er adequate andere maatregelen.

Voorzitter, dan wou ik naar de vraag van mevrouw Buitenweg over hoe ik mijn taak op het gebied van cybersecurity zie naar aanleiding van het nieuws van de afgelopen dagen over cybersecurity bij andere ministeries. Laat ik heel duidelijk zeggen dat ik het helemaal met u eens ben, mevrouw Buitenweg, dat de overheid het goede voorbeeld op het gebied van cybersecurity moet geven. Als minister ben ik coördinerend bewindspersoon, wat overigens niet wil zeggen dat ik de verantwoordelijkheid van anderen overneem. Ieder ministerie moet de eigen verantwoordelijkheid oppakken voor digitale beveiliging. Mijn collega van Binnenlandse Zaken heeft gisteren toegezegd met een brief te komen. Ik sta hierover in nauw contact met haar en zal

vanuit de coördinerende rol kijken naar acties die binnen de overheid worden uitgezet.

Mevrouw Buitenweg vroeg of er klachten van bedrijven bekend zijn over summiere wetgeving. Mijn ministerie staat veelvuldig in contact met de vitale sectoren en met de digitaledienstverleners, juist ook over het nu voorliggende wetsvoorstel en de implementatie daarvan. Daarbij zijn mij, noch mijn medebewindspersonen, tot op heden grote klachten gebleken. Voor zover er nog onduidelijkheid mocht bestaan over de precieze inhoud, kan ik de Kamer meedelen dat momenteel door de betrokken bevoegde autoriteiten én mijn ministerie wordt bezien of en in hoeverre nog nadere regels in beleidsregels of richtsnoeren moeten worden vastgelegd.

Hoe gaat de minister rapporteren over de voortgang? In de Wet gegevensverwerking en meldplicht cybersecurity is aangegeven dat we drie jaar na inwerkingtreding van de NIB-richtlijn gaan evalueren. In de tussenliggende jaren zullen we uiteraard scherp kijken naar hoe het met de implementatie gaat. Bijzonderheden over de voortgang worden in de jaarlijkse voortgangsbrief over cybersecurity meegenomen om uw Kamer verder te informeren.

De heer Van Dam vroeg of er nulmetingen komen in elke sector voor het huidige beveiligingsniveau. Het sectorale toezicht is in ontwikkeling en wordt nader vormgegeven. Het is aan de vakministers om te bepalen of in hun sector zo'n nulmeting nodig of wenselijk is. Ik wil dat écht aan hen overlaten.

De heer Rutte had een interessant idee, zeg ik eerlijk. Hij vroeg of ik bereid ben om politievrijwilligers in te zetten tegen cybercrime. Bij de politie zijn thans vrijwilligers werkzaam. Ik heb half april op een vrijdagavond een werkbezoek gebracht aan politievrijwilligers. Welnu, ik kan u verzekeren dat het buitengewoon indrukwekkend is wat mensen zonder enige vergoeding in hun vrije tijd, naast hun gewone werk, bereid zijn te verrichten voor de politie. Er zijn ook mensen die te kennen hebben gegeven over cyberexpertise te beschikken, die ze meebrengen uit hun reguliere beroep of achtergrond. Op dit moment wordt onderzocht op welke wijze we die vrijwilligers op cyber kunnen inzetten. Daarbij spelen wel zaken een rol als het vereiste screeningsniveau, de verenigbaarheid met de reguliere baan en het mogelijk moeten volgen van aanvullende opleidingen. Ik wil hardop gezegd hebben dat ik dit idee van harte zeer steun. De politie gaat er structureel mee aan de slag om te kijken hoe dat kan worden opgepakt.

De heer **Arno Rutte** (VVD):
Heel veel dank voor deze toezegging van de minister. Is de minister ook bereid om even te kijken naar het Engelse programma waarin de politie echt een aanbod aan werkgevers doet en werkgevers een aanbod terugdoen? Ze noemen dit "Employer Supported Policing". Het is echt meebewegen: we geven vrije tijd en betalen die door, waardoor dit een beetje body kan krijgen. Dat zou heel mooi zijn. De bedrijven die ik sprak, zeiden: we wachten op dat aanbod van de politie en dan gaan we meebewegen.

Minister **Grapperhaus**:
Dat gaan we zeker meenemen. We moeten de plussen van ons eigen systeem op het gebied van politievrijwilligers erbij pakken, maar natuurlijk ook kijken naar hoe anderen om ons heen dat doen.

Mevrouw Buitenweg vroeg wat ik ga doen aan informatiebeveiliging bij ministeries, dit naar aanleiding van het Verantwoordingsdebat. Daar heb ik al op gereageerd.

Mevrouw Buitenweg vroeg of het zinvol zou zijn om zo'n coördinatiemechanisme op te zetten als in de AVG is voorzien, de zogeheten artikel 29-werkgroep. Ja, de NIB-richtlijn legt veel nadruk op samenwerking tussen de lidstaten. Zo is er inmiddels een samenwerkingsgroep actief waaraan alle lidstaten, de Europese Commissie en ENISA deelnemen. Dat is artikel 11 van de NIB-richtlijn. Die richtlijn verplicht de nationale instanties op allerlei plaatsen om elkaar op de hoogte te stellen. Zij moeten ook met elkaar informatie uitwisselen over incidenten, zeker als er sprake is van grensoverschrijdende gevolgen.

Ik heb zo, dacht ik, alle vragen beantwoord.

De **voorzitter**:
De heer Van Dam is het daar nog niet mee eens.

De heer **Van Dam** (CDA):
Waar ik de minister nog niet over heb gehoord, is mijn amendement. Ik kan mij voorstellen dat hij daar in de tweede termijn op terugkomt.

Minister **Grapperhaus**:
Ik heb het hier liggen en ik moet bekennen dat het natuurlijk jammer is dat de heer Verhoeven nu op het laatste moment toch nog een Engels woord gaat gebruiken.

De **voorzitter**:
Het komt niet in de Handelingen.

Minister **Grapperhaus**:
Dat vind ik nu weer een enorme opluchting. Ik wil onmiddellijk zeggen dat ik het oordeel over het amendement aan de Kamer laat. Dat klinkt wat erg lauw, maar ik wil wel zeggen dat ik het op prijs stel dat een lid van uw Kamer heeft gekeken naar hoe we deze wet een goede Nederlandstalige benaming geven. Dat is in dit geval zeker geen overbodige luxe, zoals mijn oude moeder zou zeggen, want cybersecurity, zo merken we, is toch een moeilijk bij het publiek door te laten dringen begrip. Met een zekere mate van enthousiasme laat ik het oordeel over het amendement aan de Kamer over.

De **voorzitter**:
Dank uw wel, minister. Er staat voor de tweede termijn nog een vraag open van de heer Verhoeven over ethische hackers en een van mevrouw Buitenweg over uren en minuten. Ik kijk even naar de Kamerleden of zij behoefte hebben aan een tweede termijn. Dat is het geval. Het woord is aan mevrouw Buitenweg voor haar tweede termijn.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, voorzitter. Er lopen natuurlijk sommige onderwerpen door elkaar heen. Een aantal zaken hebben te maken met deze wet en een aantal zaken zijn daaraan gelieerd, maar worden niet helemaal besproken in die wet. Maar cybersecurity — laat ik toch het Engelse woord noemen — is natuurlijk een probleem dat wij op heel veel verschillende manieren moeten aangrijpen en waar wij als Kamer nu gelukkig veel actiever op moeten zijn. Wij zullen dus in heel veel andere debatten de behandeling van dit onderwerp moeten voortzetten.

Ik wil een lans breken voor mijn voorstel bij de minister. Dat gaat over die werkgroep, naar analogie van de artikel 29-werkgroep van de AVG. Waarom vind ik dat van belang? De minister zegt nu dat er een soort coördinatiemechanisme is waarbij we elkaar op de hoogte stellen, maar het moet natuurlijk eigenlijk verder gaan, juist om te zorgen dat er een eerlijk speelveld is — "level playing field" durf ik zeker niet te gebruiken — en dat de wetgeving op dezelfde wijze overal binnen de Europese Unie wordt toegepast. Daarmee gaat het toch iets verder. Daarom heb ik toch maar een motie voorbereid. De minister kan daar dan commentaar op geven.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de instelling van een EU-cybersecurity-werkgroep, vergelijkbaar met de WP29-werkgroep voor de AVG, eraan kan bijdragen dat de cybersecuritywetgeving in alle EU-lidstaten op dezelfde manier wordt toegepast;

verzoekt de regering in EU-verband draagvlak te zoeken voor de instelling van een EU-cybersecuritywerkgroep die zich zal inzetten voor de uniforme toepassing van de EU-cybersecurityrichtlijn,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Buitenweg. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 9 (34883).

De heer **Van Dam** (CDA):
Ik heb toch een vraag aan mevrouw Buitenweg. Uit de beantwoording van de minister heb ik begrepen dat er in Nederland jaarlijks vijftien meldingen van de ene en twintig van de andere categorie zijn. Vindt mevrouw Buitenweg het niet wat te veel van het goede om daarvoor in Europees verband een hele werkgroep, of wat dan ook, à la de AVG op te richten? De AVG is ook best wel een zwaar ingesteld fenomeen. Zou ze dat misschien nog wat nader kunnen toelichten want dat zou mij kunnen helpen bij mijn positiebepaling ten opzichte van haar motie?

Mevrouw **Buitenweg** (GroenLinks):
Ik kan de heer Van Dam zeggen dat zo'n werkgroep er in feite al zit, alleen niet helemaal met dezelfde taak. Het gaat er nu vooral om dat zaken op elkaar worden afgestemd, terwijl ik het juist van belang vind dat er gezamenlijke afspraken worden gemaakt over hoe iets moet worden geïnterpreteerd, juist ook zodat er inderdaad een gelijk speelveld is. Het is dan niet alleen helder hoe de richtlijn in Nederland maar ook in Duitsland of Italië wordt geïmplementeerd. Het is dus niet zo dat er een hele groep nieuwe mensen bij elkaar moet worden gebracht, want die is er in feite al. Die groep krijgt een nieuwe taak en het is volgens mij dan ook een beperkte aanpassing.

De **voorzitter**:
Hartelijk dank. Dan geef ik het woord aan de heer Alkaya namens de SP.

De heer **Alkaya** (SP):
Veel dank, voorzitter. In eerste termijn heb ik twee punten ingebracht. Het eerste was dat internetapparaten steeds gebruikelijker worden. Waarom zouden die niet onder de wet vallen? Het tweede is de vraag waarom de aanwijzing van de organisatie waar de meldingen van internetdienstverleners binnen zouden moeten komen, opeens per Koninklijk Besluit gaat. Bij beide antwoorden kreeg ik het gevoel dat het kabinet vooral de twee afwegingen dat we nu snel moeten overgaan tot implementatie en dat we geen nationale koppen willen, belangrijk vond. Het gaat het kabinet om snelheid en niet om de vraag hoe we deze wet zo goed mogelijk bij onze wensen kunnen laten aansluiten, zodat we een goede en duurzame wet hebben die nog jaren meekan. En dat vind ik jammer.

Ik heb dat bij die beide punten gemerkt en ook bij het punt waarop ik zojuist in mijn interrupties aansloeg, de zorg, kreeg ik een beetje datzelfde gevoel. We hebben de richtlijn erbij gepakt en in de richtlijn wordt specifiek de zorg genoemd als een mogelijke sector die bij de vitale diensten kan worden meegenomen. De minister zegt dat de zorg geen vitale dienst is omdat er ook andere opties zijn. Zo kun je ook naar een ander ziekenhuis gaan. Maar je wilt natuurlijk wel dat je patiëntengegevens door deze sector goed beveiligd worden.

Vandaar de volgende motie. Ik kan de minister geruststellen, want deze motie gaat niet over een wijziging van de wet maar juist over de algemene maatregel van bestuur. Hierdoor valt dus geen vertraging te verwachten.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat in de memorie van toelichting bij het wetsvoorstel voor de Cybersecuritywet wordt gesteld dat zorgaanbieders niet zullen worden aangewezen als aanbieders van essentiële diensten;

overwegende dat cybersecurity binnen de gezondheidszorg van cruciaal belang is voor het maatschappelijk welzijn;

verzoekt de regering in de algemene maatregel van bestuur ook zorgaanbieders aan te wijzen als aanbieder van essentiële diensten,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Alkaya. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 10 (34883).

Ik dank de heer Alkaya en geef het woord aan de heer Van Dam namens het CDA.

De heer **Van Dam** (CDA):
Dank u wel, voorzitter. Ik heb op zich geen moties en ik begrijp inmiddels ook hoe de minister aankijkt tegen mijn amendement. Toch wil ik aan de vooravond van de inwerkingtreding van de AVG van de gelegenheid gebruikmaken om nog iets te zeggen. De minister zei zelf ook al dat we in dit parlement steeds vaker over cybersecurity en de beveiliging van onze data praten.

Een tijdje terug hebben wij een hoorzitting gehouden en daar reikte iemand een prachtig beeld aan: we kunnen het als een probleem zien, maar we kunnen cybersecurity ook zien zoals we onze strijd tegen het water zien. In 1953 is er iets verschrikkelijks gebeurd, maar we hebben dat weten om te draaien in een van onze belangrijkste assets: overal op de wereld zijn er mensen uit Nederland die heel succesvol tegen het water vechten. Het is mijn hoop en ambitie om daar ook een bijdrage aan te leveren. In een land waar zo veel knooppunten van data zijn, denk ik dat we een positieve blik op het onderwerp van de beveiliging van data moeten ontwikkelen. Ik hoop dat ook deze wet daaraan bijdraagt.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan heer Arno Rutte namens de VVD. Nee, hij blijkt geen behoefte te hebben aan een tweede termijn. De heer Verhoeven namens D66 heeft dat wel. Dan is het woord aan hem.

De heer **Verhoeven** (D66):
Voorzitter, dank. Dank ook aan de minister voor de beantwoording. Aan het eind van het debat riep ik iets buiten de microfoon en de minister was in de veronderstelling dat het een Engelstalige term betrof, de term "shredder". Ik zei het overigens in het Duits. Ik had het over de "Schredder". Dus het betrof een Duitse term, want we spreken hier niet in het Engels tijdens dit debat.

De **voorzitter**:
Ook niet in het Duits overigens.

De heer **Verhoeven** (D66):
O, helaas. Nou, dan ben ik toch in overtreding geweest, voorzitter, excuus. Ik wilde dit eigenlijk als bruggetje gebruiken om aan te geven dat ik het amendement van de heer Van Dam over de naam van deze wet zal steunen. Dat is bij dezen dan ook gelijk helder.

Twee punten nog qua inhoud. Ik ga nog even kauwen op de motie van de heer Alkaya van de SP, versus, dan wel in het licht van, het antwoord van de minister met betrekking tot de zorgsector. Ik ben heel benieuwd naar het oordeel van de minister. Ik begrijp de motie van de heer Alkaya wel, maar ik moet even kijken of het antwoord van de minister voor ons voldoende geruststellend is. Ik zie wel in dat hij daarmee probeerde aan te geven dat er in de zorg wel degelijk een organisatie is om die vitaliteit voldoende te kunnen waarborgen.

Tot slot het punt van die zero-day. Ik zou daar nog even op terugkomen in tweede termijn. Dat is nu en ik doe dat toch maar gewoon via een motie. Ik dien een motie in waarmee ik de kabinetsuitzonderingen die de minister wil openhouden, niet gelijk afsluit, maar tegelijkertijd uitdruk dat ik het toch heel belangrijk vind dat het NCSC de taak voorop houdt waarvan de minister zegt dat die vooropstaat, namelijk het dichten en het helpen herstellen van onbekende fouten in software. Dat wil ik doen middels de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat het Nationaal Cyber Security Centrum de AIVD (en MIVD) in sommige gevallen van informatie voorziet over onbekende kwetsbaarheden die door ethische hackers zijn gemeld, en dat de diensten deze informatie kunnen gebruiken om te hacken;

overwegende dat een dergelijke praktijk in de weg kan staan van een veiliger internet en dat dit de positie van het NCSC kan bemoeilijken;

verzoekt de regering te bewerkstelligen dat informatie over onbekende kwetsbaarheden die door onderzoekers, ethische hackers of anderen aan het NCSC wordt gemeld, altijd wordt doorgegeven aan de maker van de software waarin de onbekende kwetsbaarheid is gevonden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Verhoeven. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 11 (34883).

De minister heeft behoefte aan tien minuten schorsing.

De vergadering wordt van 20.37 uur tot 20.45 uur geschorst.

De **voorzitter**:
Ik heropen de vergadering en geef graag het woord aan de minister.

Minister **Grapperhaus**:
Dank u wel, voorzitter. Ik had nog twee vragen openstaan voor de tweede termijn, die eigenlijk semi-eerstetermijn waren. Die kwamen op in de interrupties in de eerste termijn.

De heer Verhoeven had gevraagd naar wat we doen met die ethische hacker. Gegevens van de hacker worden door het NCSC vertrouwelijk behandeld. Er is ook contact met de hacker over het vervolg van de melding. Ik juich samenwerking met die hackers toe. Dat alles neemt niet weg dat er soms informatie aan de diensten moet worden verstrekt vanwege de nationale veiligheid. Uiteraard zal er niet meer informatie worden verstrekt dan noodzakelijk is. Ik kom straks nog terug op de motie van het lid Verhoeven.

Mevrouw Buitenweg vroeg in een interruptie in de eerste termijn: hoe snel zou je zo'n incident dan moeten melden? Kun je die termijn gelijkstellen aan die van de AVG? Dat lijkt niet wenselijk. Bij de ICT-incidenten waar dit wetsvoorstel over gaat, is het belangrijk om heel snel het eerste contact met het CSIRT en de toezichthouder te leggen. De digitale brand moet eerst geblust worden. Op dat moment zijn oorzaken vaak nog niet bekend. 72 uur kan veel te lang zijn voor het eerste contact. Je moet dus eigenlijk niet zo'n grens instellen. Je moet gewoon zeggen: zo snel mogelijk.

Mevrouw **Buitenweg** (GroenLinks):
Ik vroeg het ook omdat de minister had gezegd te gaan kijken naar één loket in plaats van drie. Ik geef aan hem mee dat daarbij bekeken moet worden dat er verschillende uurlimieten zijn.

Minister **Grapperhaus**:
Laat ik zeggen: één technisch portaal dat tot multipele meldingen kan leiden. Zo zie ik dat. Het woord "loket" vind ik misschien iets te beperkend.

Mevrouw Buitenweg had ook gevraagd: waarom niet de mogelijkheid van een soort bindend oordeel op EU-niveau zoals bij de AVG? Welnu, zo'n mechanisme zit niet in de NIB-richtlijn. Dit wetsvoorstel beperkt zich tot de implementatie van die richtlijn. Wel gaan we in de EU intensief samenwerken, zoals ik heb gezegd.

Daarmee kom ik ook meteen bij de motie op stuk nr. 9 van mevrouw Buitenweg, die ik toch echt moet ontraden. Een EU-werkgroep vind ik op dit moment nog veel te zwaar. We moeten eerst kijken hoe de lidstaten allemaal aan de slag gaan met de verplichtingen van de NIB-richtlijn en vervolgens de noodzaak en de wijze waarop gaan bepalen.

Dan is er nog een tweetal andere moties. Allereerst de motie op stuk nr. 10 van de heer Alkaya. Even het volgende. Ik heb al toegelicht waarom zorg geen vitale infrastructuur is. Maar even voor alle duidelijkheid: dat is door de minister voor Medische Zorg aangegeven. Die heeft geoordeeld: het is niet vitaal. Het is primair zijn verantwoordelijkheid. Ik vind echt: als u daar inhoudelijk over wilt gaan debatteren, dan zou dat eigenlijk separaat met hem moeten. Daarnaast zeg ik: mocht blijken dat de vakminister zegt dat iets misschien toch wel vitale infrastructuur is, bijvoorbeeld na een discussie of een debat met uw Kamer, dan zal ik het geen probleem vinden om alsnog die aanwijzing te doen. Maar er zijn in de zorg, dat wil ik nog eens benadrukken, echt al heel veel waarborgen met betrekking tot ICT-beveiliging. Men moet op dat gebied voldoen aan allerlei NEN-richtlijnen die dat waarborgen. Dat heb ik steeds gezegd. Dat is een belangrijk punt, dat maakt dat er voor mij een borging is op het punt van de zorg. Ik ontraad de motie. En ik zou de heer Alkaya dus willen suggereren om daar eventueel het debat over aan te gaan met de minister voor Medische Zorg.

De heer **Alkaya** (SP):
De minister voor Medische Zorg heeft dus aangegeven aan deze minister dat hij dat niet van vitaal belang acht. Ik vind de toelichting daarop die wij in de memorie van toelichting hebben gekregen niet afdoende. Volgens mij zouden de zorgaanbieders er wel onder moeten vallen. Zou ik de minister een plezier doen als wij op deze manier laten weten een schriftelijke toelichting van de minister voor Medische Zorg te verwachten waarin meer wordt toegelicht waarom de zorg niet onder deze wet zou moeten vallen? Dan kan ik mijn motie aanhouden en misschien dat ik me dan laat overtuigen. Het lijkt me sterk, maar ik vind dat het zoals het nu in de memorie van toelichting staat gewoon geen goed verhaal is.

Minister **Grapperhaus**:
Je moet nooit op recensies van je eigen werk ingaan, dus dat zal ik niet doen. Ik wil nog wel een keer benadrukken dat het geen vitale infrastructuur is, dixit ook de minister die daar echt over gaat en dat is die voor Medische Zorg. Het andere punt is, nogmaals, dat men al heel veel regels en richtlijnen heeft waaraan voldaan moet moet worden, waardoor er al een waarborging is. Dat heeft te maken met het specifieke karakter van die zorgsector. Ik heb in mijn eerste termijn gezegd dat als bijvoorbeeld een deel van één bepaald ziekenhuis uit zou vallen, vervanging heel goed direct mogelijk is. Dat is heel wat anders dan bij de bedrijven die echt tot de vitale infrastructuur worden gerekend. Hier wil ik het bij laten, want anders ga ik u vermoeien met herhalingen en dat moet ik niet doen.

De heer **Alkaya** (SP):
Desalniettemin ben ik van mening dat bij zorgaanbieders de veiligheid op het gebied van internet en de cyberveiligheid echt op orde moeten zijn, hoewel ik misschien ook naar een ander ziekenhuis zou kunnen gaan als één ziekenhuis uitvalt. Toch wil ik dat mijn patiëntgegevens goed beveiligd worden. Daarom denk ik dat ik mij aan mijn eigen voorstel houd. Ik houd deze motie aan. Die motie zou in principe nog in stemming gebracht kunnen worden tot november, als wij de Algemene Maatregel van Bestuur verwachten. In de tussentijd zou ik dan de voorzitter willen vragen om op deze manier een verzoek bij de minister voor Medische Zorg neer te leggen om deze commissie nadere informatie toe te sturen over waarom zorg niet onder deze wet zou moeten vallen, dus niet als vitale dienst aangewe-

zen zou moeten worden in de algemene maatregel van bestuur.

De **voorzitter**:
Ik wil de heer Alkaya adviseren om dat dinsdag bij de regeling te vragen en dan constateer ik dat hij vooralsnog zijn motie aanhoudt.

De **voorzitter**:
Op verzoek van de heer Alkaya stel ik voor zijn motie (34883, nr. 10) aan te houden.

Daartoe wordt besloten.

De **voorzitter**:
Het gaat om een specifiek verzoek aan een andere minister dan deze minister. We kunnen vragen aan deze minister of hij bereid is om dat te vragen aan de minister van Volksgezondheid. Als de minister dat toezegt, is dat in orde. Als de minister daar niet toe bereid is, zal de heer Alkaya dat volgende week bij de regeling aan de minister van Volksgezondheid moeten vragen.

Minister **Grapperhaus**:
De minister voor Medische Zorg.

De **voorzitter**:
De minister voor Medische Zorg.

Minister **Grapperhaus**:
Ik ga dat verzoek niet doorgeven en daar heb ik ook echt een beetje een principepunt in. De heer Alkaya gaat niet in op het door mij echt nou al diverse keren herhaalde punt dat echt belangrijk is, los van het punt dat de zorg niet kwalificeert voor vitale infrastructuur. Dat is overigens iets anders dan dat wij zorg, goede zorg, niet heel belangrijk vinden en dat wij de veiligheid van patiëntgegevens niet heel belangrijk vinden. Het gaat erom dat — op dat punt is niet ingegaan — de zorg heel goed zijn eigen beveiligingsregelingen heeft. Als een motie wordt aangehouden, is het niet aan mij om daar verder nog een oordeel over te geven. Een eventuele brief van de collega daar ga ik niet over. Ik heb uiteengezet dat hij het in ieder geval niet heeft gekwalificeerd. Daar wou ik het bij laten.

Voorzitter, dan wou ik naar de derde en laatste motie.

De **voorzitter**:
Meneer Alkaya, ten slotte.

De heer **Alkaya** (SP):
Het spijt me voor de minister dat hij mij niet heeft kunnen overtuigen, maar ik zal dan via de regeling het verzoek om een nadere toelichting doen aan de minister voor Medische Zorg.

De **voorzitter**:
Dank je wel.

Minister **Grapperhaus**:
Nou ja, ik had nou juist graag hier de inhoudelijke discussie gevoerd over die vraag. Ik heb gezegd: de zorg heeft die beveiliging. Als we daar niet over discussiëren, vind ik dat ook bijzonder jammer, maar dan moet dat op een andere manier.

Ik kom ten slotte op een motie van de heer Verhoeven over de onbekende kwetsbaarheden. Laat ik zeggen dat ik die motie oordeel Kamer kan laten als ik haar zo mag uitleggen dat er nog altijd een uitzondering is in die situaties waarin er naar het oordeel van het NCSC sprake is van een belang van nationale veiligheid. Dat is eigenlijk wat ik in eerste termijn ook gezegd heb. Als we het daarover eens zijn, laat ik de motie aan het oordeel van de Kamer.

De heer **Verhoeven** (D66):
Ik denk dat ik het met de minister eens ben. Die uitzondering om het aan de diensten te geven mag wat mij betreft overeind blijven, maar ik zou het prettig vinden als het NCSC het ook laat weten aan het bedrijf dat de software maakt. En dat past volgens mij precies binnen de systematiek die gebruikelijk is, namelijk dat je aan de ene kant de kans krijgt om een kwetsbaarheid te herstellen, en aan de andere kant, in het geval waarin het écht nodig is, die kwetsbaarheid ook aan een ander geeft, maar hij moet óók gemeld worden aan de maker van de software.

Minister **Grapperhaus**:
Ik heb in de eerste termijn aangegeven dat er uitzonderingssituaties denkbaar zijn waarin dat toch niet kan, op grond van de nationale veiligheid. Als ik dat kan lezen in de motie, dan kan ik haar oordeel Kamer laten.

De **voorzitter**:
De heer Van Dam heeft daar ineens een vraag over.

De heer **Van Dam** (CDA):
Voorzitter, ik besef dat ik in debat ben met de minister, maar ik hoop via wellicht drie U-bochten toch ook bij de heer Verhoeven uit te komen. Laat ik het zo zeggen: als de minister oordeel Kamer geeft, dan zou ik het, gelet op toch het enorm gevoelige element dat hier kan spelen, wel op prijs stellen als er een motie op papier staat waar we niet dingen in hoeven te lezen, maar waar de dingen gewoon in staan. Ik zou het dus enorm op prijs stellen als dan de tekst van de motie wordt aangepast, om op dat vlak werkelijk iedere twijfel weg te nemen. Dat zou het mij met dat "oordeel Kamer" wel een stuk makkelijker maken.

De **voorzitter**:
We gaan niet via de minister en de voorzitter met elkaar debatteren, maar ik wil toch de heer Verhoeven de mogelijkheid geven om hierop te reageren.

De heer **Verhoeven** (D66):
Ja. Ik snap het punt van de minister. Hij zegt: er zijn situaties waarbij de nationale veiligheid in het geding is waardoor wij onbekende kwetsbaarheden graag gemeld zien door het NCSC aan de diensten. Dat zie ik ...

Minister **Grapperhaus**:
En zelfs situaties waarin er aan de diensten wordt gemeld en het in uitzonderlijke gevallen op dat moment niet wordt gemeld aan de maker.

De heer **Verhoeven** (D66):
Dat laatste komt niet overeen met mijn motie. Ik vind een aanpassing van de motie dan te veel het gebied in duiken waar ik nou juist helderheid over wilde verschaffen. Ik zou mijn motie dus níét uitgelegd willen zien zoals de minister haar uitlegt.

Minister **Grapperhaus**:
Oké.

De heer **Verhoeven** (D66):
Dus dan zal de minister haar ...

Minister **Grapperhaus**:
Dan moet ik haar ontraden om redenen die ik uiteen heb gezet. De heer Verhoeven en ik hebben genoeg in dit debat gehoord om te weten waar het over gaat.

De **voorzitter**:
Mijnheer Verhoeven, helemaal tot slot.

De heer **Verhoeven** (D66):
Ja, en ik wil dus benadrukken dat mijn motie níét behelst het niet mogen gebruiken van die onbekende kwetsbaarheid, maar ik wil dat er tegelijkertijd een situatie ontstaat waarbij het bedrijf aan de slag kan met die onbekende kwetsbaarheid. Dan zijn er volgens mij dus twee trajecten tegelijkertijd. Maar het is nooit een traject waarbij het bedrijf dat de software gemaakt heeft niet geïnformeerd wordt ten faveure van de diensten. Dat is wat ik wil uitsluiten. Dat is een andere lezing dan die van de minister, dus dan moeten we het inderdaad helder houden, zoals de heer Van Dam heeft verzocht. Dan is de minister degene die de motie ontraadt.

Minister **Grapperhaus**:
Dat station waren we inderdaad al gepasseerd en dat is helder. Ik had u die lezing aangeboden. Het is niet zozeer mijn lezing als wel de vraag: kunnen we de motie zo begrijpen? Voorzitter, ik motiveer nog even waarom ik deze motie ontraad. Ik ontraad haar omdat er situaties kúnnen zijn waarin ... Nee, laat ik even het volgende zeggen. Deze motie is zo algemeen geformuleerd dat überhaupt de algemene uitzondering dat er een situatie kan zijn dat men aan de diensten wil melden, niet helder in de motie is opgenomen. Daarnaast sluit de motie, begrijp ik nu uit de toelichting, helemaal de situatie uit dat besloten wordt, om redenen van nationale veiligheid, de maker van de software in uitzonderingsgevallen niet die onbekende kwetsbaarheid te melden. Dat maakt dat ik de motie moet ontraden, met klem moet ontraden.

Voorzitter. Ik ben daarmee aan het eind gekomen.

De **voorzitter**:
Ik dank de minister. Daarmee is er een eind gekomen aan dit debat.

De algemene beraadslaging wordt gesloten.

De **voorzitter**:
Ik stel voor dat we dinsdag gaan stemmen over de wet, het amendement en beide moties. De minister hartelijk dank, de deelnemers hartelijk dank, de kijkers hartelijk dank. Ik wens iedereen een goede en veilige reis naar huis.