Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 084

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

Nr. 11

VERSLAG VAN EEN WETGEVINGSOVERLEG

Vastgesteld 12 oktober 2022

De vaste commissie voor Digitale Zaken heeft op 26 september 2022 overleg gevoerd met mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid, over:

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

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,
Kamminga

De griffier van de commissie,
Boeve

kst-36084-11
ISSN 0921 - 7371
's-Gravenhage 2022

Voorzitter: Leijten
Griffier: Van Tilburg

Aanwezig zijn vijf leden der Kamer, te weten: Van Ginneken, Koekkoek, Leijten, Rajkowski en Van Weerdenburg,

en mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid.

Aanvang 10.00 uur.

De **voorzitter**:
Goedemorgen. Ik open dit wetgevingsoverleg van de vaste Kamercommissie voor Digitale Zaken. We gaan het vandaag hebben over de Wet beveiliging netwerk- en informatiesystemen. Een wetsbehandeling betekent dat iedereen vrije spreektijden heeft en zoveel ruimte neemt als hij nodig heeft om de Minister en de regering te bevragen, om een goede wet met elkaar te maken. We nemen daarvoor dus de tijd. Als ik denk dat een interruptie of een gedachtewisseling ten einde is, omdat het te lang duurt of omdat alles al gezegd is, dan zal ik afhameren, maar vooraf stel ik geen regels. Iedereen heeft zelf aangegeven hoeveel tijd hij denkt nodig te hebben. Daarop hebben we gezegd dat we denken voor dit wetsvoorstel vier uur nodig te hebben. Het kan zijn dat het eerder klaar is. Als het langer doorloopt, dan denk ik, omdat iedereen andere verplichtingen heeft, dat we moeten eindigen en moeten bekijken of we de behandeling van het wetsvoorstel op een andere manier vervolgen. Ik ga daar niet van uit, maar ik wil dat toch vast zeggen.
Ik heet uiteraard de Minister van Justitie en Veiligheid welkom. Leuk dat u een keer alleen bij de commissie voor Digitale Zaken bent. Ik heet natuurlijk ook de leden van de commissie voor Digitale Zaken welkom. Aanwezig zijn vandaag mevrouw Van Ginneken van D66, mevrouw Rajkowski van de VVD en mevrouw Van Weerdenburg van de PVV. Ikzelf zal het woord voeren namens de SP. We verwachten nog het lid Koekkoek van Volt; zij zal ongetwijfeld iets vertraagd zijn. Wellicht komen er nog meerdere leden. Als dat zo is, zal ik ze welkom heten tussen de woordvoerders door.
We beginnen met de eerste termijn van de kant van de Kamer. Dat zijn de Kamerleden, die onderling uiteraard discussie kunnen voeren. Daarna zal de Minister antwoorden, zoals zo vaak: na een korte schorsing. Dan kijken we hoe we staan met het wetsvoorstel. Er zijn op dit moment nog geen amendementen ingediend op dit wetsvoorstel; dat is een wijziging van een wetsvoorstel. Maar dat kan wellicht nog komen naar aanleiding van deze beraadslagingen.
Tot zover alle procedurele mededelingen. Ik geef het woord aan mevrouw Van Ginneken van D66 voor haar eerste termijn.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter. Dank ook dat u de tijd heeft volgepraat tot ik een heerlijk kopje thee heb gekregen van de ondersteuning van de Tweede Kamer, waarvoor dank.
Voorzitter. Stel, het slot op je voordeur is kapot. Iedereen die dat weet, kan zomaar bij je binnenlopen, rondsnuffelen in je huis, je spullen stelen of je chanteren voordat je je huis terugkrijgt. De buurtwacht weet dat je slot kapot is, maar mag het je van de wet niet vertellen. De Cyber Security Raad gebruikte onlangs deze mooie analogie om te schetsen wat er mis is met de huidige regels rondom informatiedeling over kwetsbaarheden in de netwerk- en informatiesystemen van overheid en bedrijfsleven. D66 spreekt zich al een tijd uit tegen de versnippering van onze digitale weerbaarheid. Ik heb ons NCSC, ons Nationaal Cyber Security Centrum, ook al eens «Vitaal Cyber Security Centrum» genoemd, omdat deze belangrijke club digitale buurtwachters op dit moment alleen maar vitale

organisaties tegen criminelen en statelijke actoren beschermt, mag beschermen. Maar die scheiding tussen vitaal en niet-vitaal is kunstmatig en verzwakt ons allemaal. Criminelen leggen zonder dat onderscheid bedrijven plat met ransomware. Soms hebben ze enkel een financieel motief, maar zijn de maatschappelijke gevolgen vele malen groter dan hun potentiële gewin. Dat zagen we bijvoorbeeld bij het platleggen van de Colonial Pipeline in de Verenigde Staten, waardoor er in delen van de VS energietekorten ontstonden.
Omdat vaak vele bedrijven in een leveringsketen samenwerken, zijn neveneffecten van een kleine hack niet altijd meteen in beeld, maar al die afhankelijkheden maken ons gezamenlijk kwetsbaar. Cybersecurity is een gezamenlijke verantwoordelijkheid, die je dus ook in samenwerking moet organiseren. We zijn dan ook blij dat het huidige kabinet werk is gaan maken van de digitale bescherming van alle organisaties en bedrijven in ons land tegen cyberaanvallen. Daarmee beschermen we onze stabiliteit en welvaart op de korte én lange termijn. Het wetsvoorstel dat we vandaag bespreken, is dan ook belangrijk voor onze digitale veiligheid.
Voorzitter. Voor ik bij mijn vragen kom, nog even een compliment aan de Minister. Zij vroeg … De Minister kijkt heel verbaasd! Zij vroeg in mei aan onze commissie toestemming om vanwege de urgentie alvast in de geest van deze nieuwe wet te mogen handelen, door het NCSC in bepaalde gevallen dreigingsinformatie te laten delen met bedrijven en de zogeheten OKTT's. Dat zijn organisaties die vanuit hun natuurlijke plek in een bedrijfsketen of sector deze informatie snel en gericht bij hun achterban kunnen krijgen. Dat was een dappere vraag van de Minister, want als overheid moet je je natuurlijk ook gewoon aan de wet houden. D66 stelde toen onder andere als voorwaarde dat de Minister dit dan wel transparant en naspeurbaar moest doen, en vandaar ook mijn eerste vragen. Kan de Minister een korte evaluatie geven van hoe het NCSC omging met deze mogelijkheid tijdens de afgelopen maanden? En kan de Minister toezeggen om de Kamer een overzicht te geven van de aard en de ernst van de kwetsbaarheden die op deze manier gecommuniceerd zijn en welke sectoren dat betrof?
Voorzitter. Dan heb ik nog een aantal vragen over de keuzes die zijn gemaakt in dit wetsvoorstel. De Cyber Security Raad adviseert om de drempel tot het delen van informatie te verlagen van aanzienlijke gevolgen naar substantiële gevolgen. We lezen dat de Minister vreest dat de drempel te laag kan worden en dan puur gaat om financiële prikkels. Maar wat ons betreft kleven er nog wel wat zorgen aan dit antwoord. Kan de Minister iets uitgebreider toelichten waarom deze suggestie niet is overgenomen? Kan zij voorbeelden geven van de verschillen tussen aanzienlijke en substantiële gevolgen?
Ik vraag hierop door, omdat wij de geopolitieke strijd om, bijvoorbeeld, hoogwaardige technologie zien toenemen. Dat is een risico voor de toekomst van Nederland, want onze innovatie van nu is ons verdienvermogen van straks. De langeretermijneffecten van economische spionage zijn desastreus en blijven vaak jarenlang ongezien tot ze echt doordringen. Ik noemde dat daarom onlangs in ons vorige cybersecuritydebat ook een zinkgat, als ik mij dat goed herinner. Welke andere mogelijkheden ziet de Minister voor de OKTT's om bedrijven en organisaties tegen dergelijke substantiële gevolgen te beschermen? Kortom, wat kan de Minister nog doen om de OKTT's te helpen om meer te doen dan alleen paraat staan bij aanzienlijke gevolgen?

De **voorzitter**:
Mevrouw Van Ginneken, iets waar iedereen last van heeft bij dit soort wetsvoorstellen, is dat we praten in afkortingen. Wellicht is het goed voor de mensen die hiernaar luisteren en om wie het gaat, om uit te leggen wat OKTT's zijn. U heeft het even uitgelegd, maar volgens mij kunt u ook een woord gebruiken als «aanbieders» of «organisaties».

Mevrouw **Van Ginneken** (D66):
Ja, ik wil best de term «organisatie» gebruiken, maar in het wetsvoorstel is sprake van verschillende soorten organisaties en gaat het specifiek over deze OKTT. Dat zijn de organisaties die voor een sector of een bedrijfsketen een soort centrale rol vervullen en daarmee een soort schakelpunt – misschien moet ik dat woord gebruiken – kunnen zijn tussen het Nationaal Cyber Security Centrum en bedrijven en organisaties in die keten. Ik meende dat ik het om die reden even moest toelichten in mijn inleiding, maar het is heel goed dat u erop wijst dat het misschien nog iets duidelijker kon.
Voorzitter. Ik was van de weeromstuit bijna kwijt waar ik gebleven was, maar ik pak het weer rustig op. Ik lees in het wetsvoorstel dat zowel de NCSC als de Autoriteit Persoonsgegevens kijkt of deze OKTT's, deze schakelorganisaties, wel goed omgaan met de gevoelige dreigingsinformatie, want die bevat soms privacygevoelige informatie. De NCSC doet dat bij het toekennen van de zogeheten OKTT-status aan zo'n organisatie. De Autoriteit Persoonsgegevens moet vanuit haar reguliere rol toezicht houden op veilig gebruik door de OKTT's van de persoonsgegevens die in dreigingsinformatie kunnen zitten. Dit kan naar ons idee leiden tot twee kapiteins op een schip en tot onduidelijkheid voor de OKTT's. Die onduidelijkheid zou organisaties kunnen ontmoedigen om verantwoordelijkheid te nemen als OKTT. Dan blijft onze digitale weerbaarheid dus alsnog achter. Daarom heb ik de volgende vragen. Waar kijkt de NCSC nou precies naar bij het toekennen van de zogeheten OKTT-status? Waaruit bestaat de zogenoemde grondige beoordeling die de NCSC doet? Aan welke criteria wordt getoetst? Hoe verhouden die zich tot de vereisten uit de privacywet AVG? Hoe wordt na toekenning van de OKTT-status gecontroleerd of die organisaties de informatie die ze krijgen van de NCSC, niet voor onbedoelde doeleinden gebruiken? Heeft de Autoriteit Persoonsgegevens wel voldoende capaciteit om toezicht te houden op het gebruik van gegevens door deze OKTT's? Hoeveel meer toezichtswerk verwacht de Minister voor de Autoriteit Persoonsgegevens als gevolg van deze wetswijziging? En is dat apart begroot?

De **voorzitter**:
Ik heb de leden even gevraagd of het mag, maar ik stel nu een vraag ter interesse. Een van de vragen die de SP-fractie heeft, is wat we doen met de gedeelde informatie bij dreigingen. Ik doel op informatie die behulpzaam en noodzakelijk is om te delen. Maar als die informatie daar blijft liggen, verwerkt wordt of rondslingert, dan kan het ook cruciale informatie zijn om juist weer het verkeerde mee te doen. Een van de adviezen van de Autoriteit Persoonsgegevens is daarom dus ook om daar een bewaartermijn aan te geven, of om in ieder geval te verplichten die gegevens weer te verwijderen. De Minister heeft na vragen naar aanleiding van het advies van de Autoriteit Persoonsgegevens in de schriftelijke ronde aangegeven dat ze daar niet op ingaat. Zou het volgens de D66-fractie niet beter zijn als wij de Minister verzoeken dat toch te regelen, of anders zelf als Kamer het initiatief nemen om dat te regelen?

Mevrouw **Van Ginneken** (D66):
De vraag die collega Leijten stelt, is heel belangrijk. Ik heb zojuist meer breed aan de Minister gevraagd wat nou de toetsingscriteria zijn. Ik hoop in het antwoord van de Minister zeker iets te horen over bewaartermijnen. Ik kan me echter wel heel goed voorstellen dat je in deze wet niet een soort vaste bewaartermijn zou kunnen stellen, omdat het misschien ook afhangt van de aard van de dreigingsinformatie. Maar ik hoop zeker daar iets over terug te horen van de Minister en ik ben zeker bereid om er, al dan niet samen met collega Leijten, over na te denken of dat antwoord wel toereikend is.

Ik had het net over de capaciteit van de Autoriteit Persoonsgegevens. Daarover sprekend wil ik het bruggetje maken naar de blije, positieve boodschap dat het kabinet meer geld gaat uittrekken voor cybersecurity; we lazen dat in de Miljoenennota. Zo zal het NCSC 16 miljoen euro meer krijgen. Dat is een belangrijke stap richting een cyberveilig Nederland, maar tegelijkertijd groeit het takenpakket van het NCSC ook. Acht de Minister het extra geld dat naar het NCSC gaat voldoende voor de ambities van de komende jaren of voorziet de Minister een groeipad? Extra budget is natuurlijk ook nodig voor het NCSC om voldoende slimme mensen aan te kunnen trekken. Maar lukt dat ook wel echt? Zeker in dit veld is de arbeidskrapte enorm. Graag een reflectie van de Minister daarop.
Tot slot, voorzitter, kijk ik ook even naar de nabije toekomst. In Europa is er deze zomer politieke overeenstemming bereikt over de herziening van de Netwerk- en informatiebeveiligingsrichtlijn, de NIB2. Met deze nieuwe richtlijn wordt het aantal te beschermen sectoren flink uitgebreid in de hele EU. Dat is een belangrijke stap, want een keten is zo sterk als de zwakste schakel. D66 snapt dat de Minister hier niet op gewacht heeft voor de wet van vandaag, want de nu voorgestelde aanpassing is urgent. Maar datgene wat de NIB2 belooft, is dat eigenlijk ook. Ik heb dus de volgende vragen aan de Minister. Hoe snel kunnen we die volgende wijziging verwachten? Ik hoor dat de implementatie van die NIB2-richtlijn pas halverwege 2024 komt. Dat vind ik nogal laat. Vindt de Minister dat wel op tijd? Zijn er mogelijkheden om die te vervroegen?
Ik kijk uit naar de beantwoording.

De **voorzitter**:
Dank u wel, mevrouw Van Ginneken. Dan geef ik het woord aan mevrouw Rajkowski voor haar eerste termijn namens de VVD-fractie.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Uit een rapport van eerder dit jaar bleek dat 47% van de Nederlanders zich in het kader van onze nationale veiligheid het meest zorgen maakt om cyberdreigingen, gevolgd door geopolitieke dreigingen en de uitval van vitale processen. De VVD snapt deze zorgen heel goed, want als mensen door een stroomuitval niet meer kunnen pinnen of niet meer kunnen tanken of als de gehele stroomvoorziening uitvalt, dan kan dat desastreuze gevolgen hebben voor de stabiliteit van Nederland, zelfs à la minute. Ondertussen worden ook onze universiteiten, bedrijven en gemeentes dagelijks aangevallen. Helaas slaagt het cybertuig hier soms ook in. Het gevolg is dat bedrijven en gemeentes platliggen en dat er tientallen miljoenen euro's naar de cybercriminelen of naar nieuwe systemen gaan. Dat is geld dat in ieder geval niet in onze economie en samenleving gestopt kan worden. Naast het lamleggen van Nederland of het afpersen met gijzelsoftware, zijn de cybercriminelen soms ook uit op de hightechkennis die wij hier in Nederland hebben. Dat is kennis waar wij nu en in de toekomst ons geld mee gaan verdienen. Die laten wij toch niet zomaar jatten?
Voorzitter. Laten we nou het geluk hebben dat we hier in Nederland superslimme, technische mensen hebben die werken voor cyberteams van de overheid of zich op vrijwillige basis inzetten om Nederland te kunnen beschermen. Deze mensen kunnen een kwetsbaarheid in het systeem of een nieuwe manier van digitale aanvallen ontdekken. Als zij die informatie delen, kunnen we rampen voorkomen, maar die informatie kan nu alleen nog maar met een beperkte club gedeeld worden. Dat is eigenlijk een beetje ouderwets, want alles is met elkaar verbonden. Als organisatie A dus wel veilig is en informatie krijgt, maar organisatie B niet, dan kan organisatie A daar via de digitale weg ook last van krijgen, omdat die organisaties samenwerken. Het is dus allemaal een keten; mijn collega zei het net al. We moeten ervoor zorgen dat die hele keten sterk is.

Dat zien we ook wel. Zo zagen we een aantal jaren geleden dat een containerterminal in de haven van Rotterdam werd aangevallen. Dat zorgde uiteindelijk wereldwijd voor tientallen miljoenen euro's aan schade. De voedselproductie of het vervoer ervan kan ineens stil komen te liggen. Het is dus belangrijk dat we dit soort gebieden goed met elkaar beveiligen en beschermen. Daarom zijn wij zo verheugd over dit voorstel. Ook complimenten voor de snelheid en de haast die de Minister hiermee heeft gemaakt. De Kamer heeft aangegeven haast en zorgvuldigheid te willen. Volgens mij heeft de Minister laten zien, met nog extra briefings en informatie, bereid te zijn om dat te doen. Daar ben ik erg blij mee. We staan dus ook achter de oproep die de Rotterdamse haven, telecombedrijven en alle andere organisaties al eerder hebben gedaan hier in de Tweede Kamer om haast te maken met deze wet, zodat zij ook informatie kunnen gaan delen.
Voorzitter. De VVD heeft nog wel een aantal vragen, allereerst over wie er precies wanneer informatie deelt. Stel, het NCSC – dat is de club voor de vitale organisaties – heeft aanwijzingen dat er een grote kwetsbaarheid zit bij een groot maar niet vitaal bedrijf, met potentieel grote gevolgen voor onze economie en maatschappij. Heeft het NCSC dan contact met dat bedrijf, of doet het DTC dat? Dat is de club die meer werkt vanuit het Ministerie van Economische Zaken. Hoe zorgen we er nou voor dat er duidelijkheid komt over wie van de twee organisaties, het NCSC en het DTC, die beide vanuit de rijksoverheid bezig zijn met het veilig houden van Nederland, waarover met wie communiceert?
Voorzitter. Dan nog een tweede vraag. Die gaat over de rol van de vrijwilligehackersorganisatie, het DIVD. Ik noem ze maar gewoon even «de vrijwillige hackers». Dan kan iedereen het volgen. Het gaat dus over het DIVD, voor de mensen die meeluisteren. Zij hebben allemaal andere banen en werken niet bij de rijksoverheid, maar ze hebben wel aangegeven: wij willen graag Nederland veilig houden met de kennis die we hebben. Zij scannen dan ook vrijwillig op kwetsbaarheden en geven dat door aan óf een rijksoverheid óf aan bedrijven en organisaties zelf. Daarmee spelen zij een hele cruciale, maar toch ook vrijwillige rol om ervoor te zorgen dat Nederland veilig blijft. Wat de VVD nog wel mist, is wat de precieze rol is van het DIVD in het nieuwe stelsel. De andere clubs gaan daarmee samenwerken. We zouden niet willen dat deze vrijwilligehackersorganisatie echt een ambtenarenclub wordt. Dat is ook niet wat wij willen. Maar een iets formelere rol zou wat ons betreft wel mogen. Wat zijn de plannen van de Minister? Hoe gaan we ervoor zorgen dat er daadwerkelijk wat gebeurt met de informatie die deze club vrijwillig van het internet afhaalt?
Dat was het.

De **voorzitter**:
Hartelijk dank voor uw inbreng, mevrouw Rajkowski. Dan ga ik naar mevrouw Van Weerdenburg, die namens de PVV-fractie in eerste termijn zal spreken.

Mevrouw **Van Weerdenburg** (PVV):
Jazeker. Dank u wel, voorzitter. We hebben eerder een snelle behandeling van deze wetswijziging toegezegd. Daarom zal ik ook niet meer tijd dan nodig nemen. We hebben natuurlijk al een aantal keer gesproken over deze wijziging. Ook schriftelijk hebben we heel veel vragen gesteld en antwoorden gekregen. De PVV vindt deze wijziging noodzakelijk om de enorme versnippering in het cyberveiligheidslandschap, die de Cyber Security Raad natuurlijk ook gesignaleerd heeft, tegen te gaan. We denken dat dit een goede toevoeging is.
We hebben natuurlijk eerder ook in dat kader gewezen op de versnippering tussen de organisaties en er ook een beetje over gezeurd dat bekeken moet worden of het DTC en het NCSC niet samengevoegd

kunnen worden. Nogmaals, we zijn dus heel erg blij met de recente brief van de Minister, waarin zij aankondigt dat het NCSC, het DTC en het CSIRT-DSP worden geïntegreerd in de komende jaren. De PVV zal dat scherp in het oog houden. We hopen wel dat de integratie voorspoedig en snel verloopt. We rekenen ook op regelmatige berichtgeving daarover van de Minister, niet alleen als er dingen goed gaan, maar ook graag als er vertraging wordt opgelopen of er enige andere moeilijkheden zijn. Ik hoop dan dat zij ons daar proactief over informeert. We willen namelijk allemaal hetzelfde, dus laten we vooral de krachten bundelen.
Tijd is natuurlijk ontzettend belangrijk in het geval van een cyberdreiging. Het heeft ons ook altijd een beetje verbaasd dat er zo'n soort sneeuwbal was ontstaan, een soort bellijst, zo van: het NCSC krijgt het binnen, die moet de schakelorganisatie bellen, die neemt de telefoon op, die belt weer … Dat duurt allemaal te lang. Ik denk dus dat ook de integratie van de genoemde organisaties daar qua snelheid een voordeel in zal zijn.
Ik wilde positief beginnen, maar ik wil ook wel eventjes gezegd hebben dat deze route, namelijk het toepassen van de wet voordat die goed en wel is aangenomen, wat de PVV betreft niet voor herhaling vatbaar is. Dat heb ik de vorige keer ook duidelijk gemaakt, zeker aan deze Minister, want op haar terrein spelen natuurlijk ook nog andere zaken, die niet per se bij deze commissie liggen. Maar ik wilde dat hierbij gezegd hebben. Ik weet dat de Minister zelf ook heeft gezegd dat zij dit besluit niet licht genomen heeft. Zij vond het ook geen mooie oplossing. Dat heb ik allemaal goed gehoord, maar ik sluit in dat kader ook graag aan bij de vragen die D66 al heeft gesteld over de afgelopen maanden. Zo is er gevraagd of er gebruikgemaakt is van die toepassing. Dat hoor ik dus ook graag.
Mevrouw Van Ginneken had het ook over de implementatie van de NIS 2, die voorzien is voor half 2024. Zij vroeg of dat niet te laat is. Die zorg deel ik ook wel. Kunnen we dat niet versnellen? We zijn nu goed bezig en we hebben heel wat in te halen op cyberveiligheidsgebied, dus laten we ook bekijken wat we snel kunnen doen samen.
Mevrouw Rajkowski had het over de vrijwillige hackers van de DIVD. Er zijn natuurlijk nog andere goede maatschappelijke initiatieven. Ook bij de PVV leeft de behoefte om te bekijken hoe we die onmisbare vrijwilligers – in ieder geval betreft het kennis en kunde die we best wel nodig hebben – op een of andere manier beter kunnen inpassen, of formeler, zoals mevrouw Rajkowski zei. Op dit vlak moeten we alle kennis en kunde inzetten die er bestaat. Cyberaanvallen kunnen zo veel schade veroorzaken, ook voor de hele maatschappij. Laten we dus alles inzetten wat we hebben in Nederland om die schade zo veel mogelijk te beperken.
Verder heb ik...

De **voorzitter**:
Ik denk dat dit een moment is waarop mevrouw Van Ginneken een vraag wil stellen.

Mevrouw **Van Ginneken** (D66):
Ik hoorde het codewoord «verder» ook, dus daarmee sloot collega Van Weerdenburg haar blokje af. Ik wil even een vraag stellen over een punt dat bij collega Rajkowski eigenlijk ook al aan de orde kwam. Moeten we de relatie tussen de vrijwillige ethische hackers – de DIVD werd genoemd – en het NCSC niet wat formeler maken? Is mevrouw Van Weerdenburg zich ervan bewust dat veel van die vrijwilligers al werkzaam zijn in het formele veld van cybersecurity, ofwel bij een adviesbureau, ofwel bij een overheidsorganisatie en misschien zelfs wel bij het NCSC zelf? Daarover speculeer ik nu, hoor, maar ik weet dat ze in ieder geval in het professionele veld zelf ook werkzaam zijn. Zoals ik die hackers ken, vinden ze het fijn om daarnaast in een vrije rol te kunnen opereren.

De **voorzitter**:

En uw vraag is?

Mevrouw **Van Ginneken** (D66):
Dus mijn vraag is: is mevrouw Van Weerdenburg zich daarvan bewust? Waarom zou het meer formaliseren van de relatie tussen de DIVD en het NCSC helpen?

Mevrouw **Van Weerdenburg** (PVV):
Ik hoor het al: mevrouw Van Ginneken heeft inside-information, misschien meer dan ik. Kijk, ik vraag aan de Minister of dat kan en of het behulpzaam is. Als die organisaties daar geen behoefte aan hebben en beter functioneren als ze geen formele rol hebben, prima, graag zelfs. Het gaat mij er meer om dat we in ieder geval voor de maatschappij hun kennis en kunde ten volle kunnen benutten. Dat gaat uiteraard in overleg met hen. Ik vroeg me af of hier een mogelijkheid toe is als zij dat graag willen. Maar ja, als zij dit niet willen, dan gaan we dat helemaal niet verplichten. Dat lijkt me niet de goede route.

De **voorzitter**:
U kunt uw betoog vervolgen.

Mevrouw **Van Weerdenburg** (PVV):
Voorzitter. Ik geloof niet dat ik nog echt brandende vragen of punten had, maar misschien komen die lopende het debat nog op.
Dank.

De **voorzitter**:
Dan dank ik u, mevrouw Van Weerdenburg. Ik geef het woord aan mevrouw Koekkoek, die ik ook welkom heet in deze vergadering. Ik had al aangekondigd dat u waarschijnlijk iets verlaat was, maar u bent gearriveerd. Welkom. U krijgt het woord voor de eerste termijn namens de fractie van Volt.

Mevrouw **Koekkoek** (Volt):
Dank u wel. Mijn excuses voor het te laat zijn, er waren wat perikelen onderweg. Mijn eerste vraag zou gaan over de weg hiernaartoe. Er zijn al wat vragen over gesteld, dus daar sluit ik mij bij aan. Ik ben met name benieuwd, los van het gegeven dat het een unieke gebeurtenis was, of het wegingskader toereikend was, als het is gehanteerd. Ik hoop dat de Minister daar nog iets verder op in kan gaan. Hoe heeft het gewerkt als het in de praktijk is ingezet?
De Minister zegt nu dat er onverminderd sprake is van een digitale dreiging, ook in het kader van dit voorstel. Ik ben wel benieuwd wat dan die concrete dreiging is op dit moment. Op het moment dat we het eerste unieke gesprek hadden, laat ik het zo formuleren, was het met name de dreiging uit Rusland. Ik ben benieuwd of dat nog steeds zo is. Zijn er andere dingen, voor zover de Minister daarop in kan gaan uiteraard, bij gekomen? Waar bestaat die dreiging uit?
Ik heb ook nog vragen naar aanleiding van de beantwoording in het schriftelijk overleg. Er zijn namelijk een aantal pijnpunten in het wetsvoorstel. Deze zijn gedeeltelijk al benoemd door collega's. Ik heb namens Volt vragen daarover gesteld in de schriftelijke ronde. Een aantal daarvan zijn wel beantwoord, maar het is naar mijn idee nog niet helemaal helder. Ik wil de Minister daar nog wat verder over bevragen. De eerste vraag gaat over de definitie van «andere aanbieders». We hebben daar meerdere vragen over gesteld. Ik begrijp dat je die groep «andere aanbieders» open wil laten want anders heb je dadelijk een grondslag ervan die te beperkt is. Ik begrijp dat heel goed. Tegelijkertijd las ik in de reactie van de Minister dat het NCSC wel voldoende beeld heeft van met welke andere aanbieders momenteel informatie gedeeld zou kunnen

worden op grond van artikel 3, lid 2 onder e. Het gaat dan onder meer over politieke partijen en veiligheidsregio's. Omdat de Minister dat beeld dus wel heeft, vraag ik me af of de Minister een opsomming of overzicht kan geven van partijen die het NCSC momenteel in beeld heeft in dit kader. De Minister noemt ook dat de NIB-richtlijn gevolgen zal hebben voor deze wet, bijvoorbeeld vanwege een toename van het aantal aanbieders. Er is gevraagd wat de gevolgen daarvan zijn. Ik ben daar zelf ook heel benieuwd naar. Welke andere aanbieders vallen daaronder? Ik ben ook benieuwd of de verwerkingen in het voorstel zoals dat nu voorligt, wel voldoende duidelijk en voorzienbaar zijn. Dat lijkt me heel belangrijk als je wilt dat deze wet toekomstproof en duurzaam is.
Voorzitter. Ik heb in de schriftelijke ronde een aantal vragen gesteld over strafrechtelijke gegevens. De Minister schrijft dat er nu geen sprake is van strafrechtelijke gegevens, gelet op de aard van de verwerking en het feit dat de gegevens niet gebruikt worden in het strafproces of in de voorbereiding daarvan. Mijn vraag is: is het punt niet dat je juist zonder grondslag gegevens van strafrechtelijke aard mag verwerken en je die gegevens zomaar tot je beschikking hebt? Ongeacht of je ze zal gebruiken, is die kwalificatie toch van belang? Ik vraag me af of de Minister daar wat verder op in kan gaan. Volgens mij is het probleem niet dat je kennis hebt van de informatie waarover je beschikt, maar dat je niet meer onbevangen kunt handelen op het moment dat je die kennis hebt. Het simpele feit dat je die informatie hebt, kan je handelingsperspectief beïnvloeden. Vandaar dat ik daar nog wat dieper op in zou willen gaan. Om het nog even af te maken: mijn zorg is dat het feit dat je zo'n handelingsperspectief überhaupt in gedachten kunt hebben, mogelijk ook inbreuk maakt op de rechten van de verdachte. In het ergste geval wringt het met de onschuldpresumptie.

De **voorzitter**:
Daarover is een vraag van de VVD-fractie.

Mevrouw **Rajkowski** (VVD):
Ik zat even te smiespelen met mijn collega, want ik had een vraag over die strafrechtelijke gegevens. Ik begrijp het niet zo goed. Ik sla het even helemaal plat. Het gaat erover dat er informatie wordt gedeeld in de trant van: «Bedrijf A, weet dat er in deze software een deurtje openstaat. Doe een update, want daarmee zet je dat deurtje dicht. Wij zien namelijk online gebeuren dat criminelen of andere kwaadwillenden precies dat deurtje willen gebruiken.» Wat is strafrechtelijk hieraan?

Mevrouw **Koekkoek** (Volt):
Die vraag begrijp ik. Die hebben wij ook gesteld in de schriftelijke ronde. Het antwoord was toen: er is geen sprake van strafrechtelijke gegevens of die worden in ieder geval niet verwerkt. Maar als ik de AP goed begrijp, ziet zij dat risico juist wel. Je kunt potentieel te maken hebben met strafrechtelijke persoonsgegevens, want je hebt uiteindelijk wel een aanbieder in de smiezen. Het is duidelijk wie die aanbieder is, dus dan heb je potentieel te maken met strafrechtelijke persoonsgegevens. Mijn zorg is dat het op het moment dat je de kennis hebt, moeilijk is om die kennis opzij te schuiven. Ik vraag me af of je dat vermoeden niet al in dit wetsvoorstel zou willen ondervangen. Het feit dat je die kennis hebt, betekent inderdaad nog niet dat je die dan vervolgens kan delen, dus dat het bij wijze van spreken een inval van de politie zou kunnen veroorzaken. Maar het is ook wel weer heel ingewikkeld om kennis die je hebt vervolgens niet te gaan gebruiken. Ik wil dus voorkomen dat die prikkel door deze wet te open blijft. Ik vraag er vandaag even op door omdat de Minister zegt dat er überhaupt geen strafrechtelijke persoonsgegevens zijn, terwijl de AP zegt dat het risico er wel is.

De **voorzitter**:
Dank u wel. U mag uw betoog vervolgen.

Mevrouw **Koekkoek** (Volt):
Voorzitter, ik ben al bij het slot. Ik heb nu benoemd waar mijn pijnpunten zitten, maar ik wil ook benadrukken dat ik goed begrijp dat de Minister deze bevoegdheid wil inzetten. Het is ook al door andere collega's aangeven, maar de Minister ziet het volgens mij ook heel goed: er is daadwerkelijk een roep om veiligheid vanuit de praktijk. Bij mij roept het alleen het beeld op – vandaar dat ik ook die pijnpunten benoem – dat die andere kant van de medaille er ook altijd een beetje is, namelijk de veiligheid van personen en de grondrechten. Dat is een dilemma waar we met dit soort wetgeving heel vaak tegenaan lopen.
Met het oog op de toekomst hoop ik dat we ervoor kunnen zorgen dat ook wetsvoorstellen altijd vooraf – ik benadruk dat nog maar even – die balans in zich hebben, en dat we niet, zoals we nu eigenlijk doen, achteraf gaan kijken waar die balans in de wet zit. Dus ik hoop dat we er steeds beter in worden om goede wetgeving te maken vooraf. Daarin zijn stevig toereikend toezicht, afgebakende verwerkingsgrondslagen, een toets aan de grondrechten en goede ICT-voorzieningen altijd belangrijk.
Dank, voorzitter.

De **voorzitter**:
Ik dank u wel. Dan draag ik graag even het voorzitterschap over aan mevrouw Van Weerdenburg.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dan zal ik nu het woord geven aan mevrouw Leijten voor haar inbreng namens de SP.

Mevrouw **Leijten** (SP):
Dank, voorzitter. Het is belangrijk dat in wetten vastligt wat je met elkaar doet om te voorkomen dat enkelen van ons op een grote manier te maken krijgen met digitale criminaliteit, inbraken, hacks en noem allemaal maar op, want de gevolgen daarvan zijn groot. Het is evident dat de overheid daarin een coördinerende rol heeft en kan hebben, bijvoorbeeld om te waarschuwen en om, in het laatste geval natuurlijk, strafrechtelijk op te laten treden. Ik denk dat we met het stelsel dat we als Nederlandse samenleving, als politiek, hebben vormgegeven best wel ad hoc bezig zijn geweest. We hebben bijvoorbeeld het Nationaal Cyber Security Centrum, de nationaal coördinator cybersecurity; er zijn heel veel afkortingen. Die hebben we. Dat gaat over vitale aanbieders. Dan hebben we ook nog het Digital Trust Center. Dat is er gekomen voor het bedrijfsleven, want dat had ontzettend veel vragen en vroeg om hulp. Dat is er mede gekomen door heel veel inzet van deze Kamer. Nu gaan we die geïntegreerd zien. Dat is volgens de SP-fractie heel wenselijk, maar dan hebben we ook nog de AIVD. De AIVD maakt dreigingsanalyses, zeker ook op het gebied van cybersecurity. Wat is zijn rol daarin? Ik zie in de notitie die we meegestuurd hebben gekregen dat de nota en de bijgevoegde stukken allemaal afgestemd zijn met de NCTV. Wat is nou eigenlijk hún rol in dit belangrijke dossier, in wat we vastleggen in deze belangrijke wet? Wat zijn taken en verplichtingen bij dreigingssituaties, wat is de informatie die we hebben over zwaktes in netwerken en informatiesystemen en welke data delen we daarover? Dat klinkt allemaal heel saai en technisch, maar dat kan echt raken aan de vraag of je als bedrijf nog bij je gegevens kan en of je wel of niet veilig met de bank zaken kan doen.
Vindt de Minister dat dit bouwwerk, ons huis, op orde is? De SP-fractie heeft zich in de schriftelijke behandeling van dit wetsvoorstel afgevraagd

of er geen dubbeling is, maar ook of er geen gat is doordat we zoveel verschillende organisaties hebben. We hebben tegenwoordig heel veel nationaal coördinatoren, om al het beleid dat we hebben vormgegeven in allerlei wetten, te coördineren om ervoor te zorgen dat het effectief is. Maar we hebben nu een wetsvoorstel, waarin we juist kunnen regelen dat het beleid effectief is, waardoor we dus minder nationaal coördinatoren nodig hebben. Is de Minister dat met de SP-fractie eens? We moeten dus geen dingen dubbel doen, maar ook geen gaten krijgen.
Dan kom ik op die OKTT's. Ik was daar net in mijn rol als voorzitter een beetje kritisch op, omdat het een afkorting is die de SP-fractie nauwelijks begrijpt. Het zijn organisaties die objectief tot taak hebben om andere organisaties of het publiek te waarschuwen, te informeren over dreigingen en incidenten. In de wet is een lijst opgenomen van organisaties die daaronder vallen. Maar zodra je ze met afkortingen gaat aanduiden, ontstaat er afstand. Voelt iemand die misschien geen aangewezen organisatie is, die evident tot taak heeft om dit te doen, zich dan nog verantwoordelijk, ja of nee? Daardoor is het volgens mij ongewenst dat we ze in afkortingen aanduiden. Hoe wil de Minister voorkomen dat in het vervolg van dit wetsvoorstel, als het beleid gaat worden en er gegevens gedeeld gaan worden, het idee ontstaat: dat zijn wij niet, dat gaat niet over ons? Want ik denk dat het over iedereen gaat. Schakelorganisaties hebben dus voor hun achterban een signalerende, informerende en waarschuwende rol. Het zou heel goed zijn als we allemaal weten wie dat eigenlijk zijn of in ieder geval weten welke organisaties daar dan onder vallen.
Dan bespreek ik het punt van de andere organisaties. Dat is inderdaad vaag. Ik snap heel goed dat je in zo'n wetsvoorstel waarin je regelt dat de data gedeeld kunnen worden – soms moet dat snel of zijn de data moeilijk af te bakenen – zo min mogelijk regels stelt, maar toch is het de kunst dat wel te doen. Dan kan het zijn dat je vooraf misschien zegt dat het snel moet en dat je vanuit preventie moet regelen dat er niet te veel hiccups en beperkingen moeten zijn, maar zorg dan dat het toezicht goed geregeld is. En dat vindt de SP in dit wetsvoorstel echt een probleem. Het valt direct onder de Minister. De Autoriteit Persoonsgegevens waarschuwt daar eigenlijk ook voor: welke data worden er gedeeld, hoe worden die opgeslagen en hoe wordt dat ook beperkt? We weten dat we niet naïef moeten zijn als het gaat om het delen van data. We moeten zeker niet naïef zijn als het gaat over dreigingen vanuit het oogpunt van cybersecurity, maar we moeten ook niet naïef zijn als het gaat over de informatie die je krijgt en wat je daar nog mee kan doen. Ook met informatie die je wellicht ooit een keer vanuit een waarschuwing hebt gekregen en die je later weer verwerkt, kunnen hele lelijke dingen gebeuren. We willen niet dat daar profielen mee gemaakt worden. Ik zou de Minister willen vragen of zij daar toch een beperking in aan zou willen brengen. Ik zou eigenlijk de Minister willen vragen daar de eerste aanzet toe te geven. Op het moment dat de Kamer dit gaat doen in een amendement, kan het namelijk heel goed zijn dat we iets over het hoofd zien. Dan kan het ook heel goed zijn dat we iets te strak maken, waardoor de wet onuitvoerbaar wordt. Dat willen we allemaal niet. Maar ik denk dat we het signaal dat de Autoriteit Persoonsgegevens geeft – pas hier op! – serieus moeten nemen. Nu hebben we wel te maken met een wetsvoorstel waarin we dat goed kunnen regelen. Is de Minister daartoe dus bereid?
Dan bespreek ik het punt over het toezicht. We vinden het superbelangrijk dat dit beter wordt. Is het mogelijk om dat bijvoorbeeld onder een toets te scharen en mensen mee te laten kijken? Dat mag wat betreft de SP-fractie ook achteraf, want we kunnen daardoor ook leren dat we wellicht vooraf wat dingen beter kunnen regelen.
Tot slot is onze indruk dat dit wetsvoorstel is er gekomen is met stoom en kokend water. In ieder geval is het zo gepresenteerd. Het moest meteen ingaan. Daarvoor heeft de Minister toestemming gevraagd; iedereen heeft

dat genoemd. Die toestemming is uiteindelijk verleend, maar zo moeten we geen wetten maken. We moeten ook geen wetten verkopen met: er is nu oorlog, dus we moeten iets doen. Het is serieus en het gaat over ieders veiligheid, maar het gaat ook over potentieel ieders data. Het gaat wellicht over iemand die iets verkeerd heeft gedaan of iets niet voorzien heeft, maar die straks wel in een waarschuwingssysteem zit, met alle risico's van dien. Het is allemaal niet zo bedoeld en het is ook niet wat het wetsvoorstel wil behelzen, maar laten we wel zorgen dat we dit soort waarborgen en bescherming regelen. Ik vraag de Minister dus ook om als dit soort wetten nodig is, die wetten in een wat rustiger vaarwater te laten landen. De Kamer is altijd bereid om iets snel te behandelen en ook om dat op maandagochtend om 10.00 uur te doen; dat is het punt niet. Maar de argumentatie, ook in de schriftelijke ronde, klinkt als een gelegenheidsargument: het is nu nodig en het moet vooral ook nu ingaan, want oorlog. Ik zou hopen dat de Minister dat niet hoeft te gebruiken.
Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Leijten. Dan geef ik u hierbij het voorzitterschap weer terug.

Voorzitter: Leijten

De **voorzitter**:
Dan dank ik mevrouw Van Weerdenburg voor het tijdelijk overnemen van het voorzitterschap. De Minister gaat de antwoorden in eerste termijn voorbereiden. Daarom gaan we om 11.10 uur weer verder met dit debat.

De vergadering wordt van 10.40 uur tot 11.10 uur geschorst.

De **voorzitter**:
Het is 11.10 uur. Ik had gezegd dat we dan verder zouden gaan met het wetgevingsoverleg over de Wet beveiliging netwerk- en informatiesystemen. De Kamer heeft in de eerste termijn gesproken. Daarna is de Minister aan het woord. De Minister van Justitie en Veiligheid voor haar eerste termijn, met daarin de antwoorden op de vragen van de Kamer.

Minister **Yeşilgöz-Zegerius**:
Veel dank, voorzitter. Ook veel dank aan de commissie voor de voortvarende behandeling van dit voorstel. Er zijn wat vragen gesteld over het hoe en waarom en de urgentie. Daar kom ik straks ook op terug, maar nogmaals dank dat dit zo kan. Ik denk namelijk dat door de recente digitale dreigingen en aanvallen het belang echt onderstreept wordt van het in ruimere zin kunnen delen van de dreigingsinformatie en incidentinformatie door het Nationaal Cyber Security Centrum. Dit wordt nu in het wetsvoorstel geregeld.
De afgelopen jaren neemt niet alleen het aantal digitale aanvallen toe, maar ook de impact van die aanvallen. Een voorbeeld van zo'n recente digitale aanval met grote impact was een digitale aanval van vorig jaar op een ICT-leverancier van bijna 100 notarissen. Dat zijn forse zaken. Door die aanval konden er geen aktes worden gepasseerd. Als het Nationaal Cyber Security Centrum die ICT-leverancier toen had kunnen voorzien van informatie over die aanval, dan had de ICT-leverancier er maatregelen tegen kunnen nemen om die systemen te beschermen. Dat is dus echt een concreet voorbeeld van wat we in de toekomst willen vermijden of voorkomen.
Op dit moment is het nog niet altijd mogelijk om informatie over digitale dreigingen en incidenten te delen met aanbieders die buiten de huidige doelgroep van het Nationaal Cyber Security Centrum vallen. Dat gaat dus over organisaties die niet tot de rijksoverheid behoren en die we ook niet

als vitaal hebben aangewezen. Dan kunt u denken aan partijen zoals die hier zitten, dus politieke partijen, maar ook aan vakbonden, beroepsverenigingen, milieuorganisaties en noem maar op.
Voorzitter. Het fijne aan deze commissie vind ik altijd – natuurlijk geldt dat voor elke commissie – dat hier Kamerleden zitten die al zeer veel weten van het onderwerp en er langer mee bezig zijn, dus ik ga gewoon meteen door naar de beantwoording. Ik denk dat het handigst is. Ik wilde beginnen met een korte terugblik. Er zijn ook wat vragen gesteld over de afgelopen paar maanden. Maanden geleden heb ik de commissie inderdaad om ruimte gevraagd. Ik heb onszelf in een uitzonderlijke positie gebracht door te zeggen: kunnen we anticiperen als het echt nodig is? Nogmaals dank aan de commissie, die daar terecht veel vraagtekens bij zette, maar die in de basis begreep waarom we dat dilemma met elkaar hadden en dat we die stappen konden nemen. Daar ga ik dus even op in. Dan natuurlijk het wetsvoorstel. Daar komen een heleboel elementen aan bod. Dan wil ik nog stilstaan bij het cybersecuritystelsel en het Digital Trust Center. Dat waren ze. Zo heb ik ze gebundeld. Hopelijk komt dan alles terug.
Ik begin met een terugblik. Daarbij kreeg ik van mevrouw Van Ginneken en mevrouw Van Weerdenburg, of eigenlijk van iedereen, de vraag: hoe is het nou de afgelopen paar maanden gegaan, en is er gebruikgemaakt van die mogelijkheid; was het ook echt nodig? Ik heb de Kamer toegezegd dat we, met de ruimte die ik krijg, wel afspreken dat we als het is gebeurd meteen, of zodra het kan, met de Kamer delen dat dat is gebeurd. Maar sinds juni hebben die gevallen zich niet voorgedaan. Anders had ik het ook eerder moeten melden. Dat had ik dan ook gedaan. Dank voor de gelegenheid om daar nog een keer op terug te komen, maar die gevallen hebben zich niet voorgedaan. Ik heb daar dus ook geen overzicht van, want dat bestaat gelukkig niet. De drempel voor het anticiperen in uitzonderlijke gevallen ligt erg hoog. Dat hebben we ook met elkaar afgesproken. De incidenten die plaats hebben gevonden of zouden vinden die die drempel halen – het is een rare zin – zijn er niet geweest.
Dan vroeg mevrouw Koekkoek van Volt: als het wegingskader voor het eventueel anticiperen is gehanteerd, was het dan toereikend? We hadden met elkaar het volgende afgesproken. Dit is een wegingskader. We kunnen met elkaar terugkijken als het zich heeft voorgedaan. Dan kunnen we daarvan leren en het eventueel implementeren in het wetsvoorstel. Dat is allemaal niet gebeurd. Maar nu zijn we zover met het wetsvoorstel en ligt dat hier voor. Als we dan kijken naar het wegingskader en hoe dat er nu uitziet, denk ik dat dat voldoet. Het hoefde tot nu toe niet gehanteerd te worden, maar het zal wel een keer gehanteerd moeten worden, want het gaat wel verder, nu het goed geborgd wordt in de wet. Het is bedoeld om te kunnen bepalen of er sprake is van een zodanig ernstige dreiging of ernstig incident dat bij uitzondering al informatie hierover aan een aanbieder of schakelorganisatie verstrekt moet worden. Dat was de drempel voor de anticipatie, maar het wegingskader gaan we nu hier invoeren zoals we het de afgelopen maanden hadden bedacht en dat voldoet nog steeds, denk ik.
Deze vraag is voor het andere mapje van zo meteen, denk ik. Deze ook, denk ik. Dit loopt door elkaar. Ik had alleen nog een vraag van mevrouw Koekkoek, ook in het verlengde van wat mevrouw Leijten vroeg. Hier zit nogal wat urgentie op en een van de redenen dat we hier een paar maanden geleden met elkaar over spraken – dit loopt natuurlijk al veel langer; daar kom ik straks op terug – was de actualiteit in Oekraïne, met het binnenvallen door Rusland. Mevrouw Koekkoek vroeg: «Er is een digitale dreiging. Is dat nog steeds zo? Is dat alleen vanuit Rusland of zijn er nog andere dreigingen? Wat is de urgente situatie?» De ontwikkelingen in Oekraïne blijven onzekerheid opleveren; daar is helaas uiteraard niks aan veranderd. Het heeft een weerslag op de digitale veiligheid van ons land. Het Nationaal Cyber Security Centrum heeft tot op heden geen aan

de oorlog gerelateerde digitale aanvallen waargenomen, gericht op Nederlandse belangen. Momenteel lijkt het beeld daarmee stabiel, maar het dreigingsbeeld kan absoluut abrupt veranderen. We blijven het dus met elkaar in de gaten houden en het maakt alles waar we voor staan niet minder urgent. Ik denk dat dat de korte terugblik op de afgelopen paar maanden is, vanaf het moment dat we elkaar voor het laatst over dit specifieke voorstel spraken.
Dan ga ik in op het wetsvoorstel. Mevrouw Leijten had daar opmerkingen over en ik meen ook andere Kamerleden. Laat ik even stilstaan bij hoe het wetsvoorstel tot stand is gekomen. Het is natuurlijk niet zo – dat heeft ook niemand beweerd, hoor – dat we een paar maanden geleden dachten: o, we moeten wat, dus we willen nu anticiperen en we komen opeens met een wet. Het is een wetsvoorstel dat zorgvuldig is voorbereid. Het is ook in juni vorig jaar in consultatie gegaan. Toen zag de wereld er nog wel wat anders uit, maar we vonden het toen al urgent genoeg. Daarna kwamen natuurlijk alle stappen in het proces, bijvoorbeeld advies vragen aan de Autoriteit Persoonsgegevens en aan de Raad van State. Al die elementen zijn gewoon doorlopen, maar wel zo snel als we konden. We hebben dus geen stappen overgeslagen, maar we hebben wel de Kamer gevraagd het met urgentie te behandelen en dat betekent dat wij dat in huis natuurlijk ook hebben gedaan. Dat houdt in dat we alles hebben gedaan om het proces te bespoedigen. Zo hadden we de Raad van State gevraagd om spoedadvies, zoals we dat weleens doen in dit soort uitzonderlijke gevallen. Nogmaals, veel dank ook voor het snel behandelen van het voorstel hier.
Dan kom ik bij allerlei inhoudelijke vragen over het wetsvoorstel. Ik had hier van de VVD, van mevrouw Rajkowski, de vraag wie wanneer informatie deelt. Ik ga nu een paar afkortingen gebruiken en ik ga straks zeggen dat ik het volledig met mevrouw Leijten eens ben. Deze commissie weet ook van mij dat ik zelf ook helemaal knettergek word van alle afkortingen om precies dezelfde reden en ik val er ook over, maar dat is niet zo belangrijk. De afkortingen maken alles namelijk heel afstandelijk en abstract en de gemiddelde Nederlander denkt: dit gaat niet over mij, terwijl dat wel het geval is. Dat deel ik dus en ik kom er straks op terug. Ik probeer er zelf ook slagen in te maken, maar hou me aanbevolen voor alles. Bij een vorig debat heb ik alles uitgesproken en dat betekende een uur extra spreektijd voor mij! Vandaar dat ik toch af en toe op die afkortingen terugval. Maar het dilemma deel ik helemaal en dat kunnen de ambtenaren onderbouwen.
Goed, wie deelt er informatie? Stel dat het NCSC aanwijzingen heeft van kwetsbaarheden bij een groot, maar niet vitaal bedrijf. Dan heb je ook nog het Digital Trust Center, het DTC. Hoe is dan de taakverdeling onderling, nu en straks, en wie deelt wanneer wat? Het is zo dat beide organisaties momenteel ieder hun eigen primaire doelgroep hebben. De rijksoverheid en vitale aanbieders worden namelijk bediend door het Nationaal Cyber Security Centrum. Het niet-vitale bedrijfsleven wordt bediend door het Digital Trust Center. Zodra het NCSC een aanwijzing heeft van een kwetsbaarheid van een groot, maar niet vitaal bedrijf, dan geeft het die door aan het DTC. Dat betekent dat het Digital Trust Center vervolgens contact opneemt met dat bedrijf. Eigenlijk komt het erop neer dat het kan zijn dat ze voor elkaar relevante informatie hebben en dan informeren ze elkaar. Dit zijn organisaties die natuurlijk gewend zijn om vanwege de doelgroepspecifieke kennis die ze hebben opgebouwd, snel te schakelen en snel te reageren. Wij denken dat ze daardoor ook in staat zijn om de doelgroep zo goed mogelijk te bedienen en dat daardoor geen vertraging optreedt en er juist ook geen overlap is.
Het volgende is misschien ook goed om hier nog aan toe te voegen. Zij werken heel erg nauw samen en ook met de NCTV. Daar zijn ook wat vragen over gesteld, waar ik straks op terugkom. De NCTV is hierbij betrokken specifiek vanuit de coördinerende rol binnen het cybersecurity-

stelsel en als beleidsopdrachtgever van het Nationaal Cyber Security Center. Mevrouw Leijten vroeg hoe dit precies zit en hoe de rol van de AIVD en dergelijke hierin is. Dat komt nog.
Mevrouw Van Ginneken vroeg aan mij waarom ik de suggestie van de Cyber Security Raad om de drempel tot het delen van informatie te verlagen van aanzienlijke gevolgen naar substantiële gevolgen niet overneem. Met de woorden «aanzienlijke gevolgen» werpen we in ieder geval een hoge drempel op voor het delen van informatie. De kritiek kan ook zijn: té hoog. Het gaat om de continuïteit van dienstverlening. Die komt tot uiting met het begrip «aanzienlijke gevolgen». U kunt dan bijvoorbeeld denken aan een situatie waarin de systemen van een aanbieder echt uitvallen. Dat betekent dat de aanbieder daardoor de dienst niet meer kan verlenen en dat kan echt heel veel schade opleveren. Als je het hebt over substantiële gevolgen, dan verlaagt dat de drempel. Dan heb je een risico op substantiële schade. Dat kan natuurlijk heel erg heftig zijn, maar die schade kan ook financiële schade zijn of materiële schade. Nogmaals, dat is in die zin niet minder erg, maar maatschappelijke ontwrichting is er dan misschien niet. We proberen daar dus onderscheid in te maken. Daarom zeggen we in dit kader: verlaag nu niet de drempel, maar zorg ervoor dat het dan echt gaat over «gevolgen die voor de samenleving ontwrichtend zijn» – laat ik het zo samenvatten – en de meeste ernstige maatschappelijke ontwrichting.

De **voorzitter**:
Dat roept een vraag op bij mevrouw Van Ginneken. Een korte interruptie.

Mevrouw **Van Ginneken** (D66):
Ik begin met de vraag of we per blokje gaan interrumperen of direct.

De **voorzitter**:
Wat mij betreft mag u direct interrumperen, maar ik let erop dat de interrupties kort zijn omdat inleidingen niet nodig zijn. We hebben namelijk onze inbreng geleverd. Als het antwoord vragen oproept, dan is het logisch dat u daar even op reageert, maar dat hoeft bij de eerste interruptie natuurlijk niet.

Mevrouw **Van Ginneken** (D66):
Begrijp ik de uitleg van de Minister goed dat het al dan niet plaatsvinden van maatschappelijke ontwrichting hét onderscheidende criterium tussen «aanzienlijke» en «substantiële» schade is?

De **voorzitter**:
Dat is een hele mooie korte vraag.

Minister **Yeşilgöz-Zegerius**:
Ja, daar komt het op neer. Bij substantiële schade kan het ook om andere vormen van schade gaan. Nogmaals, die kunnen we met elkaar heel erg vinden en die kan ook heel erg zijn, maar die is minder fundamenteel voor de maatschappij in bredere zin. Check!

De **voorzitter**:
Dank. De Minister vervolgt haar betoog.

Minister **Yeşilgöz-Zegerius**:
Dan wederom een vraag van mevrouw Van Ginneken. Zij vroeg welke andere mogelijkheden wij zien voor de organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreiging en incidenten, de OKTT's. Ik denk dat uitspreken waar de afkorting voor staat laat zien dat soms ook het uitgesproken deel verwarrend is. Deze maakt het niet veel beter. In de verschillende

inbrengen is al heel erg goed toegelicht wat voor organisaties dit zijn. Het zijn inderdaad organisaties die bedrijven en anderen kunnen helpen om substantiële gevolgen of aanzienlijke gevolgen te voorkomen of hen daartegen kunnen beschermen.
Mevrouw Van Ginneken vraagt welke mogelijkheden zij nog meer hebben om te kunnen handelen. Deze schakelorganisaties hebben tot taak om organisaties en hun doelgroep of het publiek te informeren over de voor hen relevante digitale dreigingen, zodat zij daar op tijd op kunnen anticiperen. Het wetsvoorstel regelt dat zij in meer gevallen dreigings- en incidentinformatie van het Nationaal Cyber Security Centrum kunnen ontvangen. Zij zullen die informatie dan analyseren, waar mogelijk verrijken en daarna delen. Daar zitten dus ook nog echt wel wat handelingen. Het is niet alleen een doorgeefluik. Dat geldt ook voor informatie uit andere bronnen zoals openbare bronnen. Verder kunnen zij de informatie waarover zij beschikken, delen met het Nationaal Cyber Security Center en met andere vergelijkbare schakelorganisaties als die informatie relevant is voor hun doelgroep. Het kan dus beide kanten opgaan. Zij kunnen ook nog de samenwerking tussen organisaties in de eigen achterbannen stimuleren. Daar zitten dus een heleboel elementen in. Ik denk dat we dit daarmee goed borgen.
Ik heb de input van mevrouw Van Ginneken zo gehoord dat we dat altijd in de gaten moeten houden. Laat ik het zo zeggen. Zij vraagt niet zozeer of daarvoor per se alleen meer informatie moet worden gedeeld, want dat regelen we al, maar wel of er meer nodig is, of er behoefte is om meer te kunnen doen met die data, om die organisaties elkaar beter te kunnen laten helpen. Dat gaan we gewoon met elkaar blijven volgen, zoals we dat hier nu ook doen. Als er uit veld een duidelijke, concrete roep komt – hier moeten meer handelingen zijn; we missen iets – dan kom ik gewoon terug bij de Kamer, maar op dit moment denken we dat we dit goed hebben geborgd.
Mevrouw Van Ginneken stelde de relevante vraag wanneer je dan zo'n schakelorganisatie bent. Wanneer krijg je zo'n status? Wat is die grondige beoordeling dan en welke criteria gelden daarbij? Bij de beoordeling staat de vraag centraal of het delen van gegevens met die organisatie gerechtvaardigd en verantwoord is. Dat zijn de dingen die centraal staan. Dat betekent dat wordt getoetst of de organisatie voor de eigen systemen voldoende technische en organisatorische beveiligingsmaatregelen heeft getroffen. Daarmee wordt bepaald of de organisatie informatie van het Nationaal Cyber Security Centrum zorgvuldig verwerkt en daar vertrouwelijk mee omgaat. De manier waarop de informatie wordt ontvangen en daarmee wordt omgegaan, is dus ontzettend belangrijk om meer scherp te hebben. Er wordt ook nagegaan of de organisatie, met het oog op de vereisten van de Algemene Verordening Gegevensbescherming, maatregelen heeft genomen om die persoonsgegevens rechtmatig te verwerken. Dat is ook een vereiste. Verder wordt beoordeeld of de organisatie objectiveerbaar als taak heeft om aanbieders over digitale dreigingen en incidenten te informeren en wordt gekeken wat de doelgroep van die organisatie is. Dat laatste is een hele belangrijke factor om te bepalen of de informatie vervolgens ook voor dat doel gebruikt gaat worden. Al die elementen zijn eigenlijk de criteria aan de hand waarvan wordt getoetst of ze die status kunnen krijgen.
Dan had mevrouw Van Ginneken de vraag: hoe wordt na toekenning van die status gecontroleerd of ze het daadwerkelijk zo doen? Bij de aanwijzing als schakelorganisatie, als zogenaamde OKTT, ondertekent die organisatie een verklaring. Daarin is opgenomen dat die organisatie belangrijke wijzigingen op het gebied van een gerechtvaardigde en verantwoorde omgang met gegevens zal melden bij het Nationaal Cyber Security Centrum. Denk bijvoorbeeld aan wijzigingen met betrekking tot de getroffen beveiligingsmaatregelen, of wijzigingen van de taken en de doelgroep. Zij moeten dat dan proactief melden. Als het Nationaal Cyber

Security Centrum op basis van die melding of uit andere bronnen aanwijzingen heeft dat de gegevens niet meer gebruikt worden voor het doel waarvan wij nu met elkaar afspreken dat dat het doel is waarvoor ze gebruikt moeten worden, dan kan het NCSC die verstrekking opschorten of zelfs helemaal intrekken als dat nodig is.

Mevrouw **Van Ginneken** (D66):
Dat was een heldere toelichting van de Minister op de criteria, maar het antwoord dat ze daarvoor gaf wil ik ook even in die context meenemen. Want de criteria voor het toekennen van de status van OKTT, van schakelorganisatie, richten zich heel erg op de vraag of de processen zorgvuldig zijn ingericht. Maar de Minister zei daarvoor dat ze eigenlijk wel verwacht, of in ieder geval ziet, dat zo'n OKTT meer doet voor zo'n sector, zoals proactief informeren en informeren over informatie die binnen die sector binnenkomt. Dat zijn heel veel waardevolle dingen, denk ik. Ik zou het zonde vinden als het NCSC een OKTT aanwijst die dat allemaal niet doet, terwijl er misschien een andere organisatie is die die brede rol juist wel zou willen invullen. Het is dan zonde als het NCSC zo smal kijkt bij de beoordeling van de vraag of een organisatie OKTT-status krijgt. Sorry voor de lange inleiding, voorzitter, maar anders is mijn vraag niet duidelijk. Kan de Minister toezeggen dat ze bij de toetsingscriteria voor het toekennen van die status meeneemt of ze in bredere zin, dus buiten de dreigingsinformatie van het NCSC om, een inzet pleegt om de sector waar ze verantwoordelijk voor zijn, veiliger te maken?

Minister **Yeşilgöz-Zegerius**:
Ik denk dat dat een heel belangrijk element is. Ik begrijp de vraag zo: mevrouw Van Ginneken en ik zijn het erover eens dat het niet leidend zou moeten zijn, want dat zijn die harde criteria die de waarborg vormen voor wat we hier doen, maar dat het wel een belangrijk element is. Op die manier kunnen we het volgens mij verwerken. Ik zal dat zo even checken bij mijn ambtenaren, want anders zeg ik iets toe wat misschien niet kan. Dat kan, hoor ik. Mooi. Dat is sneller dan een antwoord in tweede termijn, zoals ik in gedachten had. Dan is het dus niet leidend, maar wel een belangrijk element voor het totaal.

Mevrouw **Van Ginneken** (D66):
Daar ben ik blij mee. Ik knikte al, maar ik maak het nu ook verbaal. Dank.

De **voorzitter**:
De Minister vervolgt haar betoog.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter.
Dat is altijd fijn voor de notulen, zeker als je aan deze kant van de tafel zit. Dan de vraag of het wel of geen extra werk is voor de Autoriteit Persoonsgegevens, want die heeft hier natuurlijk een hele belangrijke toezichthoudende rol in. Mevrouw Van Ginneken vroeg: hebben ze voldoende capaciteit, hoe ziet dat eruit? Doordat deze schakelorganisaties meer informatie kunnen ontvangen, kunnen ze meer persoonsgegevens, zoals IP-adressen, verwerken voor het uitvoeren van hun taken. IP-adressen zijn een ander soort persoonsgegevens dan waar we het hier vaker over hebben, in andere debatten, maar het zijn natuurlijk nog steeds persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op die verwerking. Wij verwachten dat dit geen grotere toezichtlast voor de Autoriteit Persoonsgegevens zal opleveren. Dat is de verwachting op dit moment. We houden het natuurlijk wel in de gaten, zoals we altijd doen, bij alle vormen van wetgeving. Als er iets in verandert, komen we erop terug. Als ik mij niet vergis, heb ik in mijn mapje ook nog wat vragen over de middelen die voor de verschillende organisaties waren vrijgemaakt.

Maar op dit moment verwachten we in ieder geval geen toename van de druk voor de AP.
Hier heb ik die vraag: extra geld voor het NCSC, het Nationaal Cyber Security Centrum. Ik hoor dat er ook nog een vraag is over de bewaartermijn, maar dat antwoord komt nog. We waren bij extra geld voor het NCSC. Daar hebben we inderdaad extra geld voor vrijgemaakt om de komende jaren te kunnen investeren in cybersecurity en om de digitale weerbaarheid van ons land, onze instanties en organisaties te kunnen vergroten. De specifieke acties en investeringen zijn opgenomen in de Nederlandse cybersecuritystrategie. Die komt medio oktober, zoals afgesproken. Daarin zullen we het ook allemaal uitschrijven. Een deel van die investeringen die volgen uit de strategie, gaat inderdaad naar het Nationaal Cyber Security Centrum. Ik denk dat het goed is om, op het moment dat die strategie gedeeld is, daar nader met elkaar over van gedachten te wisselen. U ziet het dan namelijk ook allemaal op papier. We kunnen er dan ook over praten. Het is misschien wel goed om het volgende alvast mee te geven. Ik kan me namelijk voorstellen dat dat ook in dit kader relevant is. Die investeringen in het Nationaal Cyber Security Centrum zijn wel substantieel, die zijn wel wezenlijk. Maar daar komen we dus vrij snel over te spreken.
Dan was er natuurlijk de vraag die we bij heel veel domeinen zien, en ook hier. Dat is specifiek zo bij het NCSC, maar ook in dit domein: de capaciteit. Hebben we wel genoeg mensen? Het is moeilijk om mensen te vinden. Er is sowieso sprake van krapte op de arbeidsmarkt, zeker als het gaat over dit soort specifieke kennis. Daarom heeft het Cyber Security Centrum extra geïnvesteerd in het werven van de beste mensen. Het werk wordt zo aantrekkelijk mogelijk gemaakt, er wordt goed over gecommuniceerd en men is daar heel actief in. We zien ook wel dat dat werkt. Het werpt vruchten af. Maar dat neemt niet weg dat we altijd op zoek zijn naar goede mensen. Ik zeg dat ook richting de Kamerleden. Dit is gewoon een heel belangrijk punt. Er wordt heel erg actief aan gewerkt. Alle suggesties en ideeën daarvoor zijn meer dan welkom. Dit blijft een uitdaging.

De **voorzitter**:
Een Minister die een suggestie doet dat Kamerleden een functie elders kunnen gaan zoeken, is erg kwetsbaar. De Minister zegt buiten de microfoon dat ze dat niet zou durven. Dit was ook een grap. Ik val weer terug in mijn rol als voorzitter. Mevrouw Van Weerdenburg heeft een vraag.

Mevrouw **Van Weerdenburg** (PVV):
Ja, op dit punt ben ik het eens. Het was ook mijn oproep in eerste termijn om alle kennis en kunde die er in Nederland is, in te zetten. Natuurlijk gaan we ze niet dwingen om bij de overheid te werken. Maar in dat kader zou het misschien ook een goed idee zijn, voor zover dat niet al gedaan wordt, dat het NCSC zo veel mogelijk dreigingsinformatie openbaar maakt. Dat hebben we laatst bijvoorbeeld bij de Log4J-kwetsbaarheid gezien. Het NCSC was heel snel met een GitHub. Het heeft heel veel informatie gedeeld. Die was voor eenieder te zien. Kennis en kunde die er in een samenleving is, niet bij een schakelorganisatie of wat dan ook, maar gewoon bij normale mensen die er verstand van hebben, helpt om ervoor te zorgen dat de impact van zo'n kwetsbaarheid zo klein mogelijk is. Sorry, voorzitter. Ik rond af. Zijn er nog slagen te maken? Kan er nog meer informatie openbaar gedeeld worden?

De **voorzitter**:
De laatste vraag. Het was een korte vraag.

Minister **Yeşilgöz-Zegerius**:

Ik denk dat hierbij twee elementen een rol spelen. De publiek-private samenwerking is bij dit vraagstuk natuurlijk echt cruciaal. Ik denk dat we dat binnen het cyberdomein ook heel goed terugzien. Daarbij ben ik het er volledig mee eens dat alles wat openbaar gedeeld kan worden, openbaar gedeeld moet worden. Daar moeten we ook naar blijven streven. Het wordt nu ook steeds op de website geplaatst; mevrouw Van Weerdenburg verwees er al naar. Ik denk dat alle informatie die breed van toepassing kan zijn, ook richting het veld, absoluut breed verspreid moet worden door het NCSC. Dus dat blijft ook ons verzoek, onze inzet en opdracht. Dit is dan voor de elementen die niet zomaar openbaar gedeeld kunnen worden. Daar voldoen we aan de wettelijke borging. Maar helemaal eens.

De **voorzitter**:
Dan vervolgt u uw betoog

Minister **Yeşilgöz-Zegerius**:
Ik heb hier een vraag van mevrouw Koekkoek, die volgens mij ook breder werd gesteld, wat de gevolgen van de Netwerk- en informatiebeveiligingsrichtlijn zijn voor de toename van het aantal aanbieders en welke aanbieders eronder zullen vallen. De herziening van die richtlijn is nu in de afrondende fase. Een belangrijke wijziging ten opzichte van de huidige richtlijn is dat lidstaten niet langer zelf aanwijzen welke organisaties er binnen de reikwijdte van de richtlijn vallen. In principe gaat de richtlijn gelden voor alle organisaties in een bepaalde sector, met uitzondering van microbedrijven en kleine bedrijven. Daarnaast wordt ook het aantal sectoren dat binnen de richtlijn valt, uitgebreid. Het gaat in totaal om organisaties in zeventien sectoren, zoals drinkwater, chemie en overheidsdiensten. Dus er komt inderdaad een flinke uitbreiding. Dat betekent voor ons land ook een forse toename van het aantal organisaties dat onder de richtlijn zal vallen. Het is nu in de afrondende fase. Zodra we meer duidelijkheid kunnen bieden, komt dat ook deze kant op. Maar het betekent een forse uitbreiding.
In het verlengde daarvan vroeg mevrouw Van Ginneken naar het tempo. Er staat 2024; ze vroeg of dat niet sneller moet en of dat niet een beetje laat is. Het is waar. We verwachten medio 2024 dat te kunnen implementeren. We gaan er wel van uit dat de richtlijn dit najaar wordt vastgesteld. We zijn ook afhankelijk van een aantal stappen. Bij de tijdsindicatie speelt het volgende. De richtlijn is, zoals gezegd, nog niet definitief vastgesteld. We zitten in de afrondende fase. Pas na de vaststelling weten we hoe die definitief luidt en wat die exact inhoudt. Op basis daarvan moet er een wetsvoorstel komen. We zijn dus afhankelijk van die stappen aan de voorkant. Het wetsvoorstel moet natuurlijk het hele wetgevingsproces doorlopen. Maar goed, niemand vroeg mij hier om dat te skippen. Ik zeg het maar even, want dat zijn dan de stappen die komen: de adviesaanvraag bij de Raad van State en noem maar op, en natuurlijk de behandeling in de Kamers. Ook hierbij wat mij betreft in ieder geval de afspraak dat wij aan onze kant alles zo snel mogelijk zullen doen. Dat doen we natuurlijk altijd met wetgeving, maar we snappen heel goed het verzoek om al die stappen zorgvuldig maar zo spoedig mogelijk te doorlopen. Zodra het definitief is vastgesteld, staan wij klaar om vervolgens alles op te pakken zoals we dat oppakken. Daar waar het eerder kan, zullen we het ook altijd eerder doen. Dus ik denk helemaal niet «2024, prima, geen haast», maar we moeten die stappen doorlopen. Wel goed om nog even te benadrukken dat er al voorbereidingen met alle betrokken vakdepartementen gaande zijn voor de implementatie. We doen dat op basis van de voorlopige teksten. Dus we zitten nu ook niet stil.

De **voorzitter**:
Mevrouw Koekkoek heeft hierover toch nog een vraag. Een korte vraag zonder inleiding.

Mevrouw **Koekkoek** (Volt):
Mijn vraag is of met die voorbereidende teksten in de hand nu al duidelijk is of ergens een gat zit. Het aantal verwerkingen dat nu in het voorstel ingekaderd wordt, moet duidelijk en voorzienbaar zijn. Zijn er met die tijdelijke, voorlopige tekst van de nieuwe richtlijn al gaten? Is dat voorzienbaar?

Minister **Yeşilgöz-Zegerius**:
Wat we nu al doen, is bijvoorbeeld ook met de betrokken bedrijven en sectoren dit gezamenlijk oppakken. Voor zover ik het kan overzien, loopt dat. Op het moment dat er gaten zichtbaar zijn, zullen we daar én op anticiperen én dat straks natuurlijk ook bij het voorstel betrekken en de Kamer daarover actief informeren. Op dit moment zijn we én met de vakdepartementen én de bedrijven die het betreft in voorbereiding en hebben we geen zicht op enorme gaten waarvan men zegt dat het echt om die reden zal misgaan. Dat is er niet. Maar absoluut afgesproken: als we dat wel zien, zullen we proactief daar zelf op anticiperen of in de Kamer terugkomen met dat verhaal.
Mevrouw Leijten zegt over het toezicht dat het belangrijk is dat we dat goed doen. Ze vraagt hoe het nu precies is geregeld en of er nog slimme stappen denkbaar zijn. De Autoriteit Persoonsgegevens heeft een toezichthoudende rol bij de verwerking van de persoonsgegevens door het Nationaal Cyber Security Centrum. Daarnaast houdt de Inspectie JenV toezicht op de taakuitvoering van het Nationaal Cyber Security Centrum. In dat opzicht denk ik dus dat er op dit moment al sprake is van regulier toezicht dat goed opgetuigd is en dat ook voldoende is voor hetgeen we hier vandaag bespreken. We kunnen wel kijken of de bevindingen van dit toezicht ook publiek kunnen worden gemaakt, zodat de Kamer het ook goed kan volgen en u er vervolgens ook wat van kunt vinden. Dat zullen we dan betrekken bij de gesprekken die we daarover hebben.

De **voorzitter**:
Ik heb als woordvoerder van de SP-fractie een korte vraag over het gebruik van verschillende gegevens en het verwerven van verschillende gegevens. Is er een toezichtsysteem, bijvoorbeeld in de Wiv, waarmee je vooraf toezicht vraagt maar waarmee er ook permanent toezicht is? Kan ik het zo interpreteren dat dat er is met het toezicht van de AP? Is de AP wel in staat om dat te doen? Zo niet, hoe houden we dan goed toezicht op dat wat gedeeld en verwerkt wordt en uiteindelijk achterblijft bij verschillende organisaties, of dat nou die schakelorganisaties zijn of de organisaties die nog toegevoegd worden?

Minister **Yeşilgöz-Zegerius**:
De verwijzing naar de Wiv was als voorbeeld, hè?

De **voorzitter**:
Ja.

Minister **Yeşilgöz-Zegerius**:
Want die heeft hier niets mee te maken. Ja, er is permanent toezicht door de AP, ook richting de OKTT's, de schakelorganisaties. Daar kom ik zo nog op terug, want als ik me niet vergis, was daar een vraag over. Ons beeld nu is dat de Autoriteit Persoonsgegevens dat inderdaad kan en ook doet. Ons beeld is ook dat dit past bij de rol en de ruimte en bij de capaciteit die er is.

De **voorzitter**:
Nu heeft de Autoriteit Persoonsgegevens juist gezegd dat zij vindt dat er een soort van vervaltermijn zou moeten zijn als er uitwisseling van

gegevens plaatsvindt. Dat neemt de Minister niet over. Hoe is dat dan te regelen? Hoe zit dat dan in relatie tot het toezicht?

Minister **Yeşilgöz-Zegerius**:
Laat ik dan meteen naar de vraag over de bewaartermijn gaan. Ik weet dat het hier niet door elkaar loopt, maar voor alle mensen die dit volgen is het misschien goed om het volgende nog eens te zeggen. Dit zijn persoonsgegevens, maar het zijn echt andere gegevens dan de bijzondere persoonsgegevens waarover we het vaak met elkaar hebben. De bewaartermijn gaat over de gegevens voor de organisaties die een schakelfunctie hebben. Uit de Algemene verordening gegevensbescherming volgt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel waarvoor ze worden verkregen of verwerkt. Dat is eigenlijk de afbakening. In die formulering zitten natuurlijk een paar open eindjes. Daarom kijk je per keer waar het over gaat. Deze schakelorganisaties moeten zich aan de Algemene verordening gegevensbescherming houden. Daartoe zij zijn verplicht. In hun privacybeleid moeten zij aangeven wat dan de noodzakelijke bewaartermijn is. Dat kan per incident, per dreiging verschillen. Dat maakt het lastig om het hier aan de voorkant te zeggen, plus dat ik dit niet beslis voor de OKTT's. Zij hebben hun eigen verantwoordelijkheid en moeten zich houden aan de Algemene verordening gegevensbescherming. Ze worden daar ook op gecontroleerd. Maar het kan dus ook verschillen per incident, per gegeven, noem maar op. Dit is dus al geborgd. Daarmee is het wat mij betreft niet nodig en eigenlijk niet wenselijk om dit nu alvast in de wet te regelen. Dan houd je de ruimte voor wat er echt nodig is. Ze moeten zich dus al aan de regels houden. De Autoriteit Persoonsgegevens houdt toezicht op het juist omgaan met persoonsgegevens. Daarom moet ook kunnen worden uitgelegd: waarom dit nu zo lang of zo kort? Omdat het gaat over heel veel verschillende soorten informatie is het lastig om het generiek te bepalen. Ik hoop dat ik hiermee aan de Kamerleden die daar vraagtekens bij hadden, heb kunnen uitleggen dat we niet vinden dat een bewaartermijn onbelangrijk is. Absoluut niet; die is superbelangrijk. Alleen is het op een andere manier geborgd, met – zeg ik iets te simpel samengevat in mijn woorden – iets meer maatwerk per dreiging en per soort informatie die er is.
In het verlengde hiervan had mevrouw Leijten de vraag of die informatie kan worden gebruikt voor andere doelen, zoals het maken van een profiel en dergelijke. Hoe houd je dat dan afgebakend? De Algemene verordening gegevensbescherming bepaalt al dat dat vervolgens niet voor een ander doel gebruikt mag worden. Daar zit dus die afbakening al in. Het Nationaal Cyber Security Centrum deelt alleen informatie die nodig is om een digitale dreiging weg te nemen. In de Wet beveiliging netwerk- en informatiesystemen staat dat dit het enige doel is. Voor de wetten die we vandaag bespreken, is al helemaal afgebakend dat dat het enige doel is. De AVG zegt vervolgens: je mag het niet voor een ander doel gebruiken. De aangewezen schakelorganisaties moeten verklaren dat zij de informatie die zij van het Nationaal Cyber Security Centrum ontvangen, alleen gebruiken voor het doel waarvoor het is verstrekt. Op grond van de Algemene verordening gegevensbescherming is transparantie over de verwerking van gegevens verplicht. Je hebt dus in ieder geval op verschillende niveaus en via verschillende stappen de plichten ingebouwd om dat alleen voor dat doel te gebruiken.
Laat ik de vraag van mevrouw Koekoek eerst doen, want die is in lijn met die van mevrouw Leijten. De vraag was: loop je dan vervolgens niet het risico dat je de strafrechtelijke hoek ingaat en allerlei andere zaken zonder grondslag worden gedaan met die gegevens? In het kader van het wetsvoorstel is geen sprake van persoonsgegevens over strafbare feiten zoals bedoelt in artikel 10 van de Algemene verordening gegevensbescherming. De verstrekking van gegevens gaat over bijvoorbeeld

IP-adressen, zoals gezegd. Dat is bedoeld om aanbieders in de gelegenheid te brengen om maatregelen te nemen ter bescherming van hun systemen. Ik waarschuw u, voorzitter, en dan weet u dat er een kwetsbaarheid zit in uw e-mail. Zo weet u dat u zichzelf moet beschermen, maar u weet niet dat de dreiging van mijn buurvrouw vandaan komt. Dit gaat simpel gezegd over jezelf beschermen.
Bij de enkele verwerking van bijvoorbeeld een IP-adres kan niet worden afgeleid dat er sprake is van een gedraging die een zwaardere verdenking dan een redelijk vermoeden van schuld oplevert. Ik ga nu even technisch in op de vraag van mevrouw Koekoek, die terecht technisch was. Daarvoor zijn namelijk meer concrete feiten en omstandigheden nodig dan alleen een IP-adres. Daarmee heb je het dubbel afgebakend. Dit volgt ook uit de jurisprudentie van de Hoge Raad.

Mevrouw **Koekkoek** (Volt):
Mijn zorg is meer het volgende. Stel dat je aangifte doet van een hack, wat een strafrechtelijk feit is, mag degene die een IP-adres heeft gegeven, dat adres delen met bijvoorbeeld de politie? Dan zou die informatie een strafproces inrollen.

Minister **Yeşilgöz-Zegerius**:
Ik wil even checken of we elkaar goed begrijpen. Mevrouw Koekoek krijgt informatie dat er een kwetsbaarheid is, dus dat wordt gedeeld. Dat is bijvoorbeeld een IP-adres. Het OM kan vorderen. Dan moet het OM dat IP-adres gaan vorderen. Dat kan. Die optie bestaat. Maar daar zijn al die omstandigheden en feiten nog meer bij nodig, dus alleen met het delen van het IP-adres heb je al die andere elementen niet. Om die reden is het dus afgebakend. Mevrouw Koekoek krijgt alleen dat IP-adres. Zij krijgt er niet meer context bij. Als zij daarvan aangifte doet, dan zal het OM dat moeten vorderen en vervolgens aan de slag moeten gaan om die context erbij te halen. Ik zeg het even simpel.

De **voorzitter**:
Ik zie mevrouw Koekoek. De Minister checkt en ik kijk of mevrouw Koekoek voldoende antwoord heeft, of toch een vervolgvraag wil stellen. Het mag ook in tweede termijn. U mag natuurlijk nu ook verder, ja.

Mevrouw **Koekkoek** (Volt):
Het gaat wel om informatie die je normaliter niet zou hebben. In het voorbeeld dat ik aangifte doe, zou ik die niet hebben als degene die aangifte doet. Ik zit even te twijfelen. Normaliter zou het OM dat ook niet kunnen vorderen. Daar zit dus toch informatie die je normaliter niet zou hebben in zo'n strafproceszaak. Ik begrijp dat dat IP-adres niet zo'n strafrechtelijk gegeven is, maar het wordt dan toch op een andere manier gebruikt en wordt makkelijker beschikbaar dan nu het geval is, als ik het goed begrijp.

Minister **Yeşilgöz-Zegerius**:
Ik denk dat ik de vraag begrijp. Misschien is het goed als ik daar in tweede termijn op terugkom, want dan kan ik nog iets meer context geven, bijvoorbeeld ook de jurisprudentie van de Hoge Raad, zodat we het samen beter kunnen doorgronden. Oké? Top.

De **voorzitter**:
De Minister vervolgt haar betoog.

Minister **Yeşilgöz-Zegerius**:
Dan had ik in dit mapje nog één vraag, ook van mevrouw Koekkoek. Dat betreft de vraag welke aanbieders waaraan rechtstreeks informatie kan worden gedeeld de Minister voor ogen heeft met het voorstel en welke

definities we hanteren. Het gaat om aanbieders die geen vitale aanbieder of rijksoverheidsorganisatie zijn én die niet behoren tot de doelgroep van zo'n schakelorganisatie. Daar gebruiken we drie afgebakende criteria voor. De betrokken aanbieder is niet vitaal, er is geen schakelorganisatie en er is sprake van informatie over dreiging van een incident met aanzienlijke gevolgen voor de dienstverlening van de betrokken aanbieder. Dat zijn de drie criteria. Zoals net gezegd: dan kunt u denken aan politieke partijen, vakbonden, milieuorganisaties en veiligheidsregio's. Die vallen allemaal niet onder de eerste twee criteria. Het kan aanzienlijk uit de hand lopen als het daar misgaat.

Mevrouw **Van Weerdenburg** (PVV):
Het zou natuurlijk het beste zijn als iedereen bij een schakelorganisatie aangesloten zou zijn of dat degenen die nu onder andere aanbieders vallen, misschien samen een schakelorganisatie oprichten. Is er vanuit de Minister of de overheid ook een soort stimulering om daartoe te komen? Het is noodzakelijk om de beslisboom of de sneeuwbal zo klein mogelijk te maken. Worden organisaties die nergens bij zijn aangesloten misschien ook gewezen op een bestaande schakelorganisatie?

Minister **Yeşilgöz-Zegerius**:
Daar zijn we mee bezig in de strategie die half oktober komt, want het is inderdaad zo: hoe korter en sneller de lijntjes, hoe beter. Vanuit het Nationaal Cyber Security Centrum en het DTC wordt dit gestimuleerd, maar we zullen er ook in de strategie meer aandacht aan besteden.

De **voorzitter**:
De Minister vervolgt haar betoog.

Minister **Yeşilgöz-Zegerius**:
Dan ben ik bij het mapje dat ik maar het «cybersecuritystelsel» noem. Daar vallen ook een heleboel vragen onder. Die gaan over de voorgenomen integratie tussen de diensten, tussen al die afkortingen, zoals we vorige keer zeiden. Dat is heel erg belangrijk. Het is ook een grote wens vanuit het veld en deze Kamer.
Mevrouw Van Weerdenburg vroeg: kunnen we proactief geïnformeerd worden als het goed gaat, maar ook als het niet goed gaat, zodat we het z'n allen kunnen volgen? Zeker. Ik zal de Kamer middels een brief informeren – dat hebben we ook toegezegd in de vorige commissievergadering, dus dat is een staande toezegging – over de integratie van het Nationaal Cyber Security Centrum, het Digital Trust Center en het Computer Security Incident Response Team, CSIRT. We zullen dat zeker doen. De brief zal voor aanvang van het volgende debat over onlineveiligheid en cybersecurity voor het zomerreces worden verstuurd. Ik ben het volledig eens met mevrouw Van Weerdenburg en ik hoop dat ik dat in deze commissie ook heb laten zien. Als er lastige dingen, ingewikkelde dilemma's of dingen zijn die niet goed gaan, dan deel ik dat hier. We willen hier allemaal hetzelfde. Dan kunnen we kijken waar het aan ligt en hoe we dat kunnen oplossen. Dat ga ik dus zeker doen. Ik hoop dat dit soort dingen niet gebeuren, maar anders kom ik er zeker op terug.
De vraag van mevrouw Leijten hebben we eigenlijk al besproken, maar ik vind het belangrijk om het nog maar een keer te zeggen. Ze vroeg: hoe is zo'n OKTT dan afgebakend? Daar hebben we al over gesproken, maar ze vroeg ook aandacht voor al die afkortingen en voor hoe je er nou voor zorgt dat het een toegankelijker gesprek wordt, zodat de urgentie ook duidelijker wordt. Ik wil daar echt mijn bijdrage aan leveren, ook omdat ik mezelf zie als de gemiddelde Nederlander. Die snapt het belang wel, maar het doorzien van wat er nou precies aan de hand is en wat het betekent, is gewoon heel erg complex. We zullen in de strategie dus heel veel aandacht hieraan besteden en ook ons best doen om die zo toegankelijk

mogelijk te maken. Maar laten we elkaar daar ook scherp op houden, op dit soort momenten maar ook als we met nieuwe dingen komen. Want het is geen kwestie van niet in afkortingen willen praten of geen Engelse woorden willen gebruiken. Het gaat erom dat iedereen weet: dit gaat ook over jou. Laat ik zeggen dat ik het volledig eens ben met het kritiekpunt dat dat nog niet het geval is met dit dossier. Ik moet eerlijk zeggen dat ik dat zelf ook ervaar. Dat neem ik dus absoluut mee en ik houd me ook zeer aanbevolen voor oplossingen daarin.
Dan ben ik bij de vraag van mevrouw Rajkowski en van mevrouw Van Weerdenburg over – daar gaan we weer – het Dutch Institute for Vulnerability Disclosure. Die naam hebben wij in ieder geval niet bedacht, maar het komt op hetzelfde neer; Engels en met de afkorting «DIVD». Zij vroegen: «Kan dat instituut misschien een formelere rol krijgen? Hoe zit dat eigenlijk? En hoe zorg je voor een goede samenhang?» Zo heb ik dat in ieder geval gehoord.
Het DIVD is een private organisatie. Zij heeft als doel om de digitale wereld veiliger te maken door gevonden kwetsbaarheden in digitale systemen aan mensen te melden, die die kwetsbaarheden vervolgens kunnen oplossen. Zij doet dit bijvoorbeeld door te scannen op die kwetsbaarheden. Het DIVD doet echt uitzonderlijk goed werk en daar zijn wij ontzettend blij mee. Het Nationaal Cyber Security Centrum werkt op dit moment waar mogelijk ook al heel veel samen en zal dit in het nieuwe stelsel ook blijven doen. Samenwerking tussen publieke en private partijen is gewoon cruciaal om Nederland digitaal veilig te houden, zoals ik net al zei tegen mevrouw Van Weerdenburg. Dit kun je niet vanuit één koker zelf doen. Dat bestaat gewoon niet.
Het DIVD kan op dit moment, in beginsel, door scannen binnendringen in een geautomatiseerd netwerk zonder dat daartegen een strafrechtelijk onderzoek wordt ingesteld. Het moet zich dan wel houden aan de richtlijn van het Openbaar Ministerie met betrekking tot Coordinated Vulnerability Disclosure. Daarin zijn voorwaarden opgenomen op basis waarvan binnendringen in geval van ethisch hacken niet wordt vervolgd. Daar zijn nogal strakke criteria voor. Er wordt dus gekeken of er is gehandeld in het maatschappelijk belang en dat moet men ook kunnen laten zien. Rijksoverheidsorganisaties moeten een wettelijke grondslag hebben of toestemming krijgen van de betrokken organisatie om binnen te mogen treden in geautomatiseerde netwerken, anders is er sprake van strafbaar handelen. Dat is dus best wel een verschil.
Een formele rol voor deze organisatie, het DIVD, of een samenvoeging met het Nationaal Cyber Security Centrum zorgt niet voor meer mogelijkheden voor het scannen op kwetsbaarheden. Zij hebben allemaal aparte verantwoordelijkheden daarin, want scannen zal vanuit de overheid altijd alleen maar kunnen op basis van een wettelijke grondslag. Om die reden zou ik dat dus niet nog meer bij elkaar willen voegen. Maar zoals gezegd levert het DIVD wel regelmatig informatie over mogelijk kwetsbare, geïnfecteerde en, natuurlijk, gehackte systemen aan het Nationaal Cyber Security Centrum. Het NCSC informeert vervolgens organisaties binnen hun doelgroep. Er is dus al een goede samenwerking. Wat ons betreft zullen we altijd blijven zoeken naar een betere samenwerking, want ze hebben natuurlijk wel een hele belangrijke functie.
Het lijkt erop dat ik alle vragen heb beantwoord.

De **voorzitter**:
Ik kijk even naar de collega's. Missen zij nog iets? Nee? Hebben we nog iets belangrijks gemist, griffier? Nee? Ik hou het ook in de gaten, hè.

Minister **Yeşilgöz-Zegerius**:
Daar was ik al bang voor. Dat hoort erbij.

De **voorzitter**:

Daar zijn Kamerleden ook voor, om het in de gaten te houden. Dan dank ik de Minister voor de beantwoording in eerste termijn. Ik kijk naar de Kamerleden om te zien of we door kunnen gaan naar de tweede termijn. In de tweede termijn mogen moties worden ingediend. Dat hoeft niet. Ik heb er zelf een in voorbereiding. Ik hoop dat die er op tijd is. Anders schrijf ik die nog even uit. Je weet maar nooit.
Ik geef het woord aan mevrouw Van Ginneken voor haar tweede termijn.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter. Als het uw medewerker helpt, kan ik heel veel woorden gebruiken om een heel lange inleiding te houden. Dat was ik eigenlijk niet van plan, maar ik ga mijn best doen om het niet te snel te doen.
Ik ben blij dat wij dit gesprek met elkaar hebben. Ik ben blij dat de Minister een aantal vraagpunten die ik had, heeft toegelicht. Ik ben gerustgesteld dat het NCSC de informele bevoegdheid om informatie te delen de afgelopen maanden niet nodig heeft gehad. Maar to the point: ik ben blij dat de Minister heeft toegezegd de schakelorganisaties, de OKTT's, actief te stimuleren om een bredere rol te vervullen dan alleen het verspreiden van de informatie die ze van het NCSC krijgen. Wie mij wat langer kent, weet dat ik de rol van brancheorganisaties, die zomaar zo'n OKTT zouden kunnen zijn, altijd aanjaag. Zij kunnen in het algemeen meer doen dan nu om onze economie en samenleving te beschermen. Dit is daar een invulling van. Ik ben blij dat de Minister heeft toegezegd dat actief in de toetsingscriteria op te nemen. Ik heb nog wel één zorg die ik wil delen. Misschien kan de Minister daarop nog reageren. Zij zei dat de Autoriteit Persoonsgegevens door dit wetsvoorstel geen extra werk krijgt. In principe vergroot elk wetsvoorstel waarbij een nieuwe gegevensverwerking tot stand komt het terrein waarop de AP werkt. In dit geval vind ik dat het wat extra aandacht vraagt, want het gaat om organisaties die soms nieuw zijn, en die in ieder geval een hele nieuwe taak gaan vervullen. Dat is een belangrijke, maar ook gevoelige taak, want het gaat om tot personen herleidbare gegevens. Daarbij heeft de Minister ook aangegeven dat die organisaties zelf allerlei keuzes maken in hoe ze hun proces inrichten, maar ook in hoe zij bijvoorbeeld omgaan met bewaartermijnen. Dat vind ik dan eigenlijk toch wel kwetsbaar, omdat je een situatie instapt waarbij heel veel organisaties dingen voor het eerst gaan doen. Kan de Minister ingaan op de mogelijkheid dat de Autoriteit Persoonsgegevens actief alle OKTT's die worden ingesteld, gaat visiteren en bekijken om te zien hoe het is ingericht? Dan kunnen die organisaties zelf en de Autoriteit Persoonsgegevens daarvan ook leren, zodat we zeker weten dat we met elkaar het goede aan het doen zijn. Als het antwoord daarop ja is, kan de Minister de Kamer dan over die bevindingen informeren?
Dat was mijn tweede termijn, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Van Ginneken. Dan geef ik het woord aan mevrouw Rajkowski, die spreekt namens de VVD.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Dank ook aan de Minister voor haar beantwoording over de groep ethische hackers. RTL Nieuws noemde ze laatst «hackers met goede bedoelingen». Dat vond ik eigenlijk ook wel leuk, dus misschien kunnen we ze ook wel zo noemen.
Ik zie toch nog wel een probleem voor ze. Ik ben namelijk op zoek naar het volgende. Als het gaat om een formelere rol voor het DIVD, bedoel ik niet dat zij een rijksoverheidslabeltje moeten krijgen. Maar nu krijgen zij bijvoorbeeld alleen maar incidenteel geld, en ik zou liever zien dat ze structureel geld krijgen. Daar ga ik hier nu geen voorstel voor doen, maar dit is alvast een winstwaarschuwing dat ik zo in de wedstrijd zit. Daarnaast zou ik ook willen dat het oppakken en doorspelen van de informatie over

dreigingen die zij hebben, een structurelere vorm krijgt. Voor deze groep hackers is het namelijk ook niet altijd duidelijk. Als ze informatie aan de rijksoverheid geven, komt die niet altijd bij die bedrijven terecht. En wie gaat die bedrijven dan helpen om verder door te groeien met die informatie? Ik merk dat de schoen daar nog wringt. Wij zijn er in die zin voor dat het een formelere organisatie wordt. Het moet geen rijksoverheidsorganisatie worden, maar wat zij doen mag nog wel iets meer richting en serieusheid krijgen. Daarom wil ik de volgende motie indienen.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat Nederland dagelijks onder vuur ligt door cyberaanvallen op zowel vitale als niet-vitale bedrijven;

overwegende dat met het actief scannen op kwetsbaarheden bij aanbieders veel cyberaanvallen tijdig kunnen worden voorkomen;

constaterende dat zowel het Nationaal Cyber Security Centrum als het Digital Trust Center krachtens de Wet beveiliging netwerk- en informatiesystemen gericht zijn op dreigingsinformatie delen en adviseren over het nemen van maatregelen aan vitale en niet-vitale aanbieders;

constaterende dat het Dutch Institute for Vulnerability Disclosure op grotendeels vrijwillige basis het internet proactief scant op kwetsbaarheden en deze meldt bij relevante aanbieders;

verzoekt de regering te onderzoeken op welke wijze het Dutch Institute for Vulnerability Disclosure een grotere, formele rol kan gaan spelen in het digitaal veilig houden van Nederland in samenwerking met het NCSC en het DTC,

verzoekt de regering uiterlijk in het voorjaar van 2023 de Kamer te informeren over de uitkomsten van dat onderzoek en de eventuele opvolging van die uitkomsten,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Rajkowski.
Zij krijgt nr. 9 (36 084).
De bode neemt de motie over. Ik zal u als voorzitter zeggen dat die onderdeel uitmaakt van de beraadslaging. U zag mij een beetje moeilijk kijken omdat ik me afvraag of de motie echt bij het wetsvoorstel past. Maar u heeft het er wél over gehad, dus we gaan die gewoon toevoegen aan de beraadslaging. Ik denk altijd aan de fracties die niet aanwezig zijn en de discussie hebben gemist. Kunnen zij dan afwegen hoe ze moeten stemmen? Maar we laten de motie gewoon aan deze vergadering toevoegen. Dan kan de Minister reageren. We stemmen over anderhalve week, dus ik hoop dat dat dan voldoende tijd geeft. Mevrouw Van Weerdenburg, ik geef u het woord voor de tweede termijn namens de PVV-fractie.

Mevrouw **Van Weerdenburg** (PVV):

Dank u wel, voorzitter. Ik dank de Minister voor alle antwoorden. Nogmaals, de PVV is blij met deze wetswijziging, omdat die in onze ogen bijdraagt aan het tegengaan van de versnippering in het cyberveiligheidslandschap. In dat kader kijken we natuurlijk reikhalzend uit naar de cybersecuritystrategie. Nog maar negentien nachtjes slapen! We verwachten daar gewoon veel van, zeg ik in de richting de Minister. Ik herinner haar ook even aan de belofte dat ze er een heel mooi uitgetekend organogram bij zou doen om het visueel ook meteen duidelijk te maken. Ik zie haar nu wel lichtelijk bezorgd kijken, maar wie weet. U heeft nog een paar weken.
De motie over het DIVD van de vorige spreker vind ik wel sympathiek. Omdat die natuurlijk ook idealiter ingepast moet worden in de cybersecuritystrategie, denk ik dat het relevant is.
Voorzitter. Verder hadden wij geen opmerkingen. Dank.

De **voorzitter**:
U ook bedankt, zeg ik tegen mevrouw Van Weerdenburg. Dan geef ik het woord aan mevrouw Koekkoek voor haar tweede termijn.

Mevrouw **Koekkoek** (Volt):
Dank, voorzitter. Ik heb ook niet zo heel veel, eigenlijk. Het was een goed debat. Het is mooi als de punten een beetje overeenkomen, dus de pijnpunten die de Kamer ziet en de punten waar de Minister op reageert. Dat is altijd prettig, vind ik. Waar ik vooral heel blij mee ben, is de toezegging van de Minister om, met betrekking tot de NIB-richtlijn en de criteria die we nu gebruiken voor de relevante aanbieders, het meteen met de Kamer te delen op het moment dat er iets misgaat of risico's ontstaan. Ik denk dat dat met name belangrijk is voor de aanbieders zelf, want je moet je kunnen voorbereiden. Eigenlijk is het tijdpad best wel kort tussen het ingaan van deze wet en het implementeren van die richtlijn. Ik denk dus dat dat heel belangrijk is.
Op het punt van de strafrechtelijke gegevens komt de Minister straks terug. Zodat het straks sneller gaat, zal ik wel alvast meegeven waarom op dat punt voor mij een zorg zit. Dat is namelijk omdat we, misschien onbewust, extra gegevens via deze wet in een strafproces kunnen brengen. Dan kan je zeggen «nou goed, je moet überhaupt niet hacken» – daar ben ik het mee eens – maar we moeten ervoor oppassen dat op het moment dat data verzameld worden, die bewust, onbewust of halfbewust worden ingezet voor iets waar ze eigenlijk niet voor bedoeld zijn. Dat zou eventueel in deze wet opgevangen moeten worden, maar ik kan me ook voorstellen dat we dat juist in de regels omtrent het strafprocesrecht op moeten vangen. Soms hebben bepaalde ingrepen ten aanzien van data op andere plekken een effect dat je niet altijd ziet aankomen. Ik geef nu alvast mee dat daarin mijn zorg zit. Ik hoop dat de Minister daar straks in de tweede termijn op in kan gaan.

De **voorzitter**:
Mevrouw Rajkowski met een vraag.

Mevrouw **Rajkowski** (VVD):
Als ik haar net goed heb gehoord, heeft de Minister aangegeven dat dit wettelijk gezien al geregeld is. Dat gaat onder andere om de AVG, maar ook om allerlei andere verordeningen. Die afbakening zit er dus al in, ook in deze wet. Informatie mag alleen gebruikt worden voor dit doel en niet strafrechtelijk. In de AVG staat dat ook. Ik ben er een beetje naar op zoek wat Volt dan nog extra wil gaan regelen. Als het al heel duidelijk in meerdere wetten vastgelegd staat, is het volgens mij meer zaak om daarop te handhaven en te controleren dan om nog meer wetten te gaan maken. Is Volt dat met mij eens?

Mevrouw **Koekkoek** (Volt):
Als het makkelijk kan, ben ik daar in principe helemaal voor. Maar waar nu mijn zorg in zit, is waar ik net naar vroeg. Ik noem even het voorbeeld waarin ik de aanbieder ben die gehackt wordt en informatie krijg over een IP-adres. Dat gebied is afgebakend; dat erken ik ook. Maar wat mij logisch lijkt, is dat ik als aanbieder dan vervolgens aangifte doe van een hack, een strafbaar feit. Op dat moment heb óf ik beschikking over een IP-adres, waar ik dat vóór het ingaan van deze wet niet zou hebben, óf het OM zou dat kunnen vorderen, wat normaliter ook niet zou kunnen, omdat je die informatie dan niet hebt. Dan komt dus toch via – laten we zeggen – een zijpad informatie in het strafprocesrecht, waar je dat voorheen niet zo makkelijk tot je beschikking zou hebben. Mijn zorg zit erin dat dat misschien per ongeluk gaat, onbewust. Ik denk dat je er als wetgever sowieso altijd van op de hoogte moet zijn welke informatie je beschikbaar stelt. Een tweede zorg is natuurlijk dat je dan wellicht toch de rechten van een verdachte ondermijnt. Nogmaals, ik vind niet dat je moet hacken en het moet inderdaad allemaal simpel kunnen, maar ook daarvoor geldt: rechten van een verdachte zijn er niet voor niks.

De **voorzitter**:
Ik hoorde mevrouw Rajkowski «dank» zeggen. Mevrouw Koekkoek, u bent aan het einde van uw betoog? Ja. Dan geef ik even het voorzitterschap over aan mevrouw Van Weerdenburg.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan mevrouw Leijten voor haar tweede termijn.

Mevrouw **Leijten** (SP):
Dank daarvoor. Ik denk zeker dat het een goed debat was. Het is een belangrijke wet, die richting geeft en een afwegingskader dat al gebruikt wordt wettelijk vastlegt. Er moet de SP-fractie wel iets van het hart over het anticiperen op de wet. Dat moest, en daarover hebben we snel nog een debat gevoerd omdat we dachten: het is wel een uitzonderlijke situatie dat dit niet is toegepast. Dat laat bij de SP-fractie wel een beetje een smaak achter in die zin dat daarbij wellicht argumenten zijn gebruikt of een sfeer is gecreëerd die iets te hoogdravend zijn geweest. Niettemin leggen we het nu vast. Daarbij zegt de Minister: eigenlijk voldoen het toezicht en de wettelijke basis die we al hebben wel als het gaat over de waarborgen die er zijn. De SP-fractie denkt dat dit zo is. Tegelijkertijd staan we aan de vooravond van toch wel een behoorlijke verbouwing van toezicht, signalering, het in de gaten houden. Er gebeurt natuurlijk ook heel veel. Er is internationale dreiging en nationale dreiging. Er gebeurt heel veel op het internet waardoor we de aanpak daarvan moeten verbeteren. Onze zorg is dat juist het toezicht op wat we doen en op het delen en verwerken van gegevens bij al die uitdagingen en ambities het kind van de rekening wordt. Het gaat dan om de vraag wat er bewaard blijft, wat voor risico's dat heeft in de toekomst, of dat nou strafrechtelijk is of niet, en de vraag of het wordt opgeslagen in profielen. Dat is allemaal niet de bedoeling en het is allemaal nu niet voorzien, maar je weet het niet. Daarom heb ik een motie geformuleerd, die ik op papier heb gekregen, waarvoor heel veel dank aan degene die de motie heeft gebracht. Ik heb er zo min mogelijk argumenten in gezet, want het gaat echt om het bieden van een soort waarborgfunctie. Het is ook geen oordeel, alsof de Minister het niet goed genoeg geregeld zou hebben, maar meer een soort stok achter de deur.

De Kamer,

gehoord de beraadslaging,

constaterende dat de Minister aangeeft dat toezicht en bescherming van gegevensverwerking bij de Wet beveiliging netwerk- en informatiesystemen (36 084) voldoende is vormgegeven;

verzoekt de regering bij de evaluatie van de wet en/of het wegingskader specifiek aandacht te besteden aan toezicht op het delen van de gegevens, de verwerking en het bewaren daarvan,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Leijten.
Zij krijgt nr. 10 (36 084).

Mevrouw **Leijten** (SP):
De context ervan is dat een wet altijd wordt geëvalueerd. Dit wegingskader wordt misschien wel vaker geëvalueerd, omdat dit ook werkende weg beter kan worden. Er zit ook nog best wel wat in ministeriële regelingen dat buiten ons als medewetgever geregeld kan worden. De oproep in deze motie is eigenlijk om het toezicht daarop altijd goed te evalueren en goed te beschouwen.
Nogmaals, de gedachte is niet dat de Minister daar geen oog voor heeft of geen oog voor zou willen hebben. Maar wat de SP-fractie betreft is dit wel belangrijk om altijd op het netvlies te houden. Nou hoorde ik net van mijn collega van de PVV dat we inderdaad heel snel de cybersecuritystrategie van dit kabinet krijgen. Zij weet nog secuurder hoeveel uur, minuten en dagen dat nog zal duren en ook dat daar nog een goede verdeling bij zit, maar ik zou de Minister op het hart willen drukken om daar ook de rol van zowel de NCTV als de AIVD goed bij te betrekken. Ik had daar wat vragen over gesteld. Die zijn niet heel erg beantwoord. Dat geeft niet voor nu. Maar het idee is dat we nu iets wettelijk regelen vanuit de juiste bedoelingen. Tegelijkertijd zijn er veel organisaties en is er veel bestuurlijke drukte. Daardoor blijft de angst dat we dingen dubbel gaan doen of juist dingen vergeten, omdat dat net niet iemands taak is. Dat kan met zo'n overzicht of strategie ook ondervangen worden. De oproep van de SP is dus om daar aandacht aan te besteden.
Bedankt.

De **voorzitter**:
Dank u wel, mevrouw Leijten. Ik zie geen interrupties. Ik geef u dus het voorzitterschap weer terug.

Voorzitter: Leijten

De **voorzitter**:
Dan dank ik mevrouw Van Weerdenburg. Wij gaan over drie minuten verder. Dan is de Minister klaar voor de beantwoording in tweede termijn.

De vergadering wordt enkele ogenblikken geschorst.

De **voorzitter**:
Ik geef de Minister van Justitie en Veiligheid het woord in tweede termijn.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Ik wil vooral nog ingaan op de twee moties en de vraag die ik nog van Volt heb staan. Ik heb alle andere elementen meegeschreven en die nemen we gewoon mee. Dat zeg ik nu maar even, want we spreken al heel snel verder met elkaar over cybersecurity.
Ik behandel eerst de moties. De eerste motie op stuk nr. 9 van de VVD verzoekt of we kunnen kijken hoe we het Dutch Institute for Vulnerability Disclosure, het DIVD, een fundamentelere rol kunnen geven. Ik hoor mevrouw Rajkowski duidelijk zeggen dat ze snapt dat het dan niet per se gaat om een formele rol als onderdeel van het hele stelsel zoals we het nu hebben. Zoals ik net al aangaf zie ik dat ook eigenlijk niet zitten. Maar ze zegt wel: ze doen zo belangrijk werk, dus kijk dan hoe dat beter geborgd kan worden. Vanuit dat idee geef ik deze motie oordeel Kamer.
Ik heb de inleiding van de motie op stuk nr. 10 van mevrouw Leijten goed gehoord. Ze zegt: ik zoek met alle kennis van nu op tig domeinen en dossiers een extra waarborg, een verankering eigenlijk, van wat de Minister heeft gezegd. Zo zie ik het. Beide moties krijgen wat mij betreft oordeel Kamer.
Dan heb ik nog de vraag van mevrouw Koekkoek. Dat is een ingewikkelde en een simpele vraag tegelijk. Dat is altijd lastig. Daar kom ik nu achter. In principe, heel sec gezien, heeft zij gelijk. Laten we daarbij beginnen. Dat is altijd de beste openingszin. Stel dat mevrouw Koekkoek die informatie heeft gekregen, een IP-adres bijvoorbeeld. Het kan ook haar eigen IP-adres zijn. Stel dat zij van een ander de informatie heeft gekregen dat daar een kwetsbaarheid in zit en dat ze daar alert op moet zijn. Zij zegt: «Daar kan ik dus aangifte van doen. Dan heb ik gegevens die ik anders niet had gehad.» Dat kan vervolgens het begin zijn van een onderzoek of van een strafrechtelijk iets. Feitelijk is het zo dat dat kan. Het OM kan die gegevens ook bij het NCSC vorderen. Zij kunnen het overal vorderen. Maar de kans dat het per se bij één aangifte met een IP-adres begint, is wel heel klein. Laten we even vanuit dat scenario doorwerken. We zien – dat komt terug in de jurisprudentie maar ook in andere voorbeelden waarbij dat niet kan – dat de informatie waarmee dan aangifte wordt gedaan zo weinig is, dat het OM vervolgens wel allerlei andere feiten en context erbij zal moeten gaan vinden om ook echt zo'n proces te kunnen beginnen. Alleen op basis van de informatie die mevrouw Koekkoek heeft gekregen, zul je hoogstwaarschijnlijk niet meteen een zaak hebben. Maar goed, je kunt nooit alles uitsluiten. Zo zit het. Het is geen gegeven in het strafproces, maar het zou er wel aanleiding toe kunnen geven. Maar dan nog moet het OM een rond verhaal hebben. Dat zou in een uitzonderlijk geval kunnen, maar als Minister van JenV zou ik daar het volgende aan willen toevoegen, ook al was dat niet de vraag. Als het OM het verhaal rond kan maken, dan is dat mooi meegenomen, maar dat is niet het doel. Ik snap heel goed waarom ze daarop doorvraagt. Al die afbakeningen zijn verankerd. Het zou in een uitzonderlijk geval kunnen, maar je mist dan nog steeds heel veel feiten en context. Alleen op basis van een IP-adres kun je geen strafrechtelijk onderzoek starten. Ik denk dat dat het antwoord was.

De **voorzitter**:
Ik kijk naar de collega's en zie geen nadere vragen. Ik dank de Minister voor haar aanwezigheid en de beantwoording over dit wetsvoorstel. Ik dank uiteraard ook de leden voor de behandeling van dit wetsvoorstel, de mensen hier in de zaal, de ondersteuning, de griffier, de stenograaf, de bode en de mensen die dit thuis allemaal hebben gevolgd. Dat geldt ook voor alle ambtenaren, zo zegt de Minister terecht. Ook belangrijk om te weten: op 4 oktober stemmen we over dit wetsvoorstel en de ingediende moties.

Sluiting 12.18 uur.