Verslag van een commissiedebat

De vaste commissie voor Digitale Zaken heeft op 11 april 2024 overleg gevoerd met mevrouw Adriaansens, minister van Economische Zaken en Klimaat, over **Onlineveiligheid en cybersecurity**.

De fungerend voorzitter van de vaste commissie voor Digitale Zaken,
Kathmann

De griffier van de vaste commissie voor Digitale Zaken,
Boeve

Voorzitter: Kathmann
Griffier: Muller

Aanwezig zijn vijf leden der Kamer, te weten: Kathmann, Rajkowski, Six Dijkstra, Valize en Van der Werf,

en mevrouw Adriaansens, minister van Economische Zaken en Klimaat.

Aanvang 13.00 uur.

Aan de orde is de behandeling van:
- de brief van de minister van Economische Zaken en Klimaat d.d. 16 juni 2023 inzake reactie op verzoek commissie over het RDI-rapport over storingsproblematiek en cybersecurity van omvormers voor zonnepanelen (26643, nr. 1038);
- de brief van de minister van Justitie en Veiligheid d.d. 26 juni 2023 inzake integratie Digital Trust Center, CSIRT-DSP en Nationaal Cyber Security Centrum (26643, nr. 1058);
- de brief van de minister van Justitie en Veiligheid d.d. 3 juli 2023 inzake Cybersecuritybeeld Nederland 2023 (26643, nr. 1045);
- de brief van de minister van Justitie en Veiligheid d.d. 3 juli 2023 inzake samenhangend inspectiebeeld cybersecurity vitale processen (26643, nr. 1046);
- de brief van de minister van Economische Zaken en Klimaat d.d. 12 juli 2023 inzake voortgang van de activiteiten van het ministerie van Economische Zaken en Klimaat (EZK) met betrekking tot de aanlanding van nieuwe onderzeese datakabels en het vitaal

verklaren van onderzeese datakabels (26643, nr. 1060);
- de brief van de minister van Economische Zaken en Klimaat d.d. 18 september 2023 inzake voortgang moties mkb-keurmerk en een structurele cyberoefenagenda voor niet-vitale bedrijven (26643, nr. 1068);
- de brief van de minister van Justitie en Veiligheid d.d. 9 oktober 2023 inzake voortgang Nederlandse Cybersecuritystrategie (26643, nr. 1072);
- de brief van de minister van Justitie en Veiligheid d.d. 8 februari 2024 inzake WODC-rapport Evaluatiekader en nulmeting Nederlandse Cybersecuritystrategie (NLCS) (26643, nr. 1128);
- de brief van de minister van Economische Zaken en Klimaat d.d. 8 maart 2024 inzake voortgang Digital Trust Center en het Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP) (26643, nr. 1143);
- de brief van de minister van Economische Zaken en Klimaat d.d. 8 april 2024 inzake beleidsreactie onderzoek contractuele afspraken cybersecurity (26643, nr. 1148).

De **voorzitter**:
Ik denk dat we van start kunnen. Het is precies 13.00 uur. De mensen zitten hopelijk al klaar voor dit debat Onlineveiligheid en cybersecurity. Welkom aan al mijn collega's en in het bijzonder aan de minister. Gezien de tijd die we hebben, denk ik dat we niet heel erg streng hoeven te zijn. Maar we moeten het toch een beetje afbakenen, dus ik stel voor dat we het aantal interrupties zetten op vier in twee. Daar moeten we wel mee uit de voeten kunnen, denk ik. Ik deel eerst nog mee dat mevrouw Rajkowski gelukkig in ons midden is, maar dat ze zich misschien zo weer even moet excuseren om naar een ander debat te rennen. Daarna komt ze waarschijnlijk terug. Het woord is aan u.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Dat gebeurt als je iets kleiner bent als partij na de verkiezingen, maar we gaan het doen.

Voorzitter. Onlineveiligheid en cybersecurity. De VVD zet zich in voor een vrij, veilig en welvarend Nederland in de fysieke wereld, maar ook online. Onze samenleving wordt steeds meer afhankelijk van digitalisering. Dat brengt economische voordelen mee -- kijk maar naar onze fintech-economie en welvaart -- maar het maakt ons ook enorm kwetsbaar. Eén succesvolle

cyberaanval, één incident in een bedrijf of organisatie kan al snel leiden tot een domino-effect en uiteindelijk een uitval bij bijvoorbeeld gas, water, elektra of een hele supply chain van een voedselketen. Het is vandaag, vanochtend ook erg actueel dat bedrijven eigen alarmsystemen en alarmcodes niet op orde hebben.

Voorzitter. De VVD heeft de afgelopen jaren meerdere voorstellen gedaan om het mkb en de inwoners van Nederland te beschermen. In dit debat wil ik drie punten naar voren brengen: analoge terugvalopties, veiligheid van het mkb en de zonnepanelen en omvormers.

Eerst de analoge terugvalopties. Daar heb ik samen met de Partij voor de Dieren vorig jaar nog een motie voor ingediend. Dank ook voor de brief en de uitvoering daarvan. Nu wordt eigenlijk elk jaar in Aanpak vitaal ook gekeken hoe het zit met de weerbaarheid van onze vitale sector en hoe analoge terugvalopties die weerbaarheid kunnen verhogen. Dat is fijn; dat volgen we op de voet. Het wordt ook alleen maar actueler. NAVO-topman Rob Bauer adviseerde dat de Nederlanders een zaklamp, drinkwater en dat soort dingen in huis hebben, niet alleen bij een digitale aanval maar ook gewoon bij een storing. Het is de inzet van de VVD geweest dat ook de rijksoverheid haar analoge plannen en haar eigen drinkwater klaar heeft staan. Dus dank. Geen vraag, maar ik wilde dit nog even benoemen.

Dan de veiligheid van het mkb. Mkb'ers denken nog te vaak dat een cyberaanval hen niet zal overkomen. Maar op het moment dat een mkb'er vastzit in een digitale gijzeling, kan dat potentieel het faillissement van het bedrijf betekenen en ook een persoonlijke ramp. Daarom breken wij een lans voor het helpen van de mkb'ers in hun strijd tegen cybercriminaliteit. Hierbij is het ook belangrijk dat het DTC zijn dienstverlening sneller uitbreidt om nog meer informatie, ook ongevraagd, aan nog meer mkb'ers te geven. We horen namelijk van VNO dat dit nog beter en sneller kan. Graag een reactie hierop van de minister.

Daarnaast willen we de minister complimenteren voor het snel opvolgen van onze verzoeken over een cybersecuritykeurmerk en om daarin ook aan te haken op Europese ontwikkelingen. Dat is heel fijn. Je wil niet nog een los keurmerk, maar kijken naar alles wat er al loopt. Het geldt ook voor het aanbieden van de cyberoefeningen voor mkb'ers.

Dan het laatste punt, de zonnepanelen en omvormers. Steeds meer mensen hangen hun dagelijks leven aan het internet -- laat ik het maar zo zeggen -- dus ook spullen thuis. Als deze apparaten niet veilig zijn of niet veilig worden gemaakt, geïnstalleerd en beheerd, dan zijn mensen erg kwetsbaar voor kwaadwillenden. De toezichthouder, de RDI, maakt zich ernstig zorgen om een groot deel van de omvormers voor zonnepanelen op de markt. Het bleek dat bijna alle omvormers die ze hebben onderzocht niet veilig zijn. Daardoor kunnen ze storing veroorzaken, op afstand uit worden gezet, gehackt worden, maar ook als onderdeel van een cyberaanval als een wapen worden ingezet. We kunnen niet verwachten dat als mensen dit soort technologische snufjes in huis halen, zij allemaal begrijpen hoe ze daarmee om moeten kunnen gaan. Daar ligt dus ook echt een verantwoordelijkheid voor de fabrikant, voor de verkoper, maar ook voor degene die dit beheert. De RDI adviseert om een omvormer alleen maar aan te schaffen als er een CE-markering op staat, want anders voldoet die niet aan de veiligheidseisen. Vanaf 1 augustus dit jaar gaan er nieuwe veiligheidseisen gelden. Dat is erg fijn. Alleen betekent dit dat tussen nu en 1 augustus mensen alsnog zijn overgeleverd aan de goodwill van de fabrikanten of de installateurs, dus dat mensen die nu zonnepanelen aanschaffen of laten installeren alsnog onveilige apparaten in huis halen. Graag een reactie hierop.

(vervolg - loopt door, beurtnummer 2) Mevrouw **Rajkowski** (VVD):
Ook al gaan die wettelijke eisen pas vanaf de zomer in, wat de VVD betreft doet de minister er nu alles aan om ervoor te zorgen dat mensen gerust de klimaattransitie kunnen aangaan.

Dank.

De **voorzitter**:
Ik zie verder geen interrupties. Het woord is aan de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):
Dank u wel, voorzitter. Laten we het eens over China hebben: een mooi land met een rijke historie en een cultuur van hartelijkheid en gastvrijheid, maar ook een land met een staatsinrichting die op veel vlakken diametraal tegenover die van Nederland staat. De scheiding van overheid en markt zoals we die in Nederland kennen, bestaat niet op die manier in China en er is geen echte tegenmacht. Chinese bedrijven moeten doen wat de overheid ze opdraagt, of het nu gaat om het overhevelen van data of om het inbouwen

van achterdeurtjes in Chinese apparatuur en software. China heeft een lange adem en diepe zakken en heeft bovendien de ambitie om wereldleider te worden.

Intellectueel eigendom stelen uit andere landen via cyberspionage blijkt bijvoorbeeld geen probleem in China, van vliegtuigontwerpen tot halfgeleidertechnologie. Naar buiten toe wordt het glashard ontkend, maar al jarenlang is vastgesteld dat deze diefstal door de Chinese overheid niet alleen wordt getolereerd, maar zelfs gestimuleerd, gefinancierd en gecoördineerd. Dit alles zal de minister niet onbekend in de oren klinken. De AIVD-jaarverslagen zijn al jarenlang glashelder over de intenties en cybercapaciteiten van China. Afgelopen februari hebben de MIVD en het NCSC nog actief openbaar gemaakt dat de Chinese malware Coathanger op systemen van het ministerie van Defensie is ontdekt. Hulde voor deze transparantie overigens.

We, parlement en regering, kunnen gezamenlijk wel vaststellen dat de cyberdreiging vanuit China reëel is. Daar moeten we als Nederland weerbaar tegen zijn, en dat zijn we vaak nog onvoldoende. De minister van JenV rapporteert zelf in de voortgang op de NLCS dat het volgens de toezichthouders noodzakelijk is om de cyberbasishygiëne te verbeteren en het risicomanagementproces naar een hoger niveau te tillen. Dat lijkt me heel verstandig, maar toch. De minister van JenV geeft in haar beantwoording van eerdere Kamervragen van mijn kant aan dat het kabinet een landenneutraal beleid voert als het gaat om leveranciers van netwerkapparatuur en dat het gebruik van Chinese routers en switches binnen kritieke omgevingen daarbij niet bij voorbaat uitgesloten is. Hoe houdbaar is dat landenneutrale beleid nog? Wordt het niet tijd om dat beleid eens te gaan herzien en de veiligheidseisen op te schroeven? Of laat ik 'm omdraaien: onder welke omstandigheden zou het volgens de minister wel verantwoord zijn om Chinese edge devices, dus apparaten die netwerken met het internet verbinden, in kritieke omgevingen te gebruiken?

De minister zegt verder in haar beantwoording dat, om eventuele risico's van het gebruik van routers en switches te kunnen beheersen, het van belang is te bepalen welke rol deze hebben in de infrastructuur. Dat klinkt op zich natuurlijk heel logisch, maar uiteindelijk gaat het in de cyberveiligheid om de zwakste schakel, en routers en switches hangen aan het internet. Een aanvaller hoeft niet alle routers en switches te kunnen hacken; eentje is voldoende om binnen te komen. En als hij eenmaal binnen is, ook al is dat in

een relatief onbelangrijk gedeelte van een netwerk, kan hij vanaf daar doorstappen naar andere, kritieke delen. Hoe meer edge devices in je netwerk zitten, hoe groter het aanvalsoppervlak en hoe kwetsbaarder je dus bent.

Daarbij moet je uiteraard verder kijken dan enkel het land van herkomst van de apparatuur. Het edge device dat door Chinese actoren gehackt was in de Coathangercasus betrof een firewall van een Amerikaans merk dat om de haverklap kritieke kwetsbaarheden lijkt te hebben. Is de minister het met mij eens dat als je China en andere statelijke actoren buiten de deur wilt houden, het juist de edge devices zijn waarvan je verzekerd moet zijn dat deze veilig zijn? Is er niet veel terrein te winnen door in het aankoop- en aanbestedingsproces voor kritieke infrastructuur nationale veiligheid niet zomaar een overweging te laten zijn, maar het primaire uitgangspunt? Wat is het standpunt van de Taskforce Economische Veiligheid hierin? Gaan de NIS2, de Cyber Resilience Act of de ABRO nog iets veranderen aan de situatie zoals die nu is? En hoe zorgen we ervoor dat dit security-firstprincipe niet alleen een papieren werkelijkheid is binnen overheidsstrategieën, maar ook bij de uitvoering?

Daarmee kom ik bij mijn laatste punt. Nederland gaat de implementatiedeadline van de NIS2-wetgeving helaas niet halen, zoals het er nu naar uitziet. Laat ik het zo zeggen: het is bepaald niet de eerste Europese wet waarvoor dat geldt. Mijn vraag aan de minister is: hoe komt dat? Is er misschien ook een oorzaak te vinden in het feit dat de Nederlandse verantwoordelijkheid voor cybersecurity bij zo veel verschillende partijen belegd is, in tegenstelling tot in andere EU-landen zoals Duitsland en Frankrijk, waar er één duidelijke cyberautoriteit is voor de verschillende taken binnen beleid en uitvoering? Is hier ooit een vergelijkende analyse op gedaan?

Ik zie uit naar de beantwoording. Dank u wel.

De **voorzitter**:
Er is een interruptie van mevrouw Rajkowski van de VVD.

Mevrouw **Rajkowski** (VVD):
Fijn om NSC ook in deze commissie te hebben. Als ik het zo hoor, denk ik: daar kunnen we wel zaken mee doen op dit thema. Het gaat inderdaad niet alleen om het kunnen uitsluiten van bepaalde apparaten. Is NSC het met de

VVD eens dat mensen of bedrijven moeten weten dat ze dat kunnen? Ik heb voor mijn verlof, een halfjaartje geleden, iemand van een gemeente op de lijn gehad. Die zei: wij moeten nieuwe camera's gaan inkopen, wij willen graag Chinese camera's uitsluiten om de plekken waar we ze gaan hangen, maar onze juristen zeggen dat dat niet kan. Ze moesten zelfs allerlei advocatenkantoren inhuren om te onderzoeken of dat wel of niet mogelijk was. Ik zei: mij is altijd verteld dat wij wet- en regelgeving niet hoeven aan te passen, want je kan ze op grond van nationale veiligheid al uitsluiten. Volgens mij gaat het er niet alleen om dat je de wettelijke kaders scherp hebt, maar ook dat alle overheidsinstanties weten wat die kaders zijn en waar ze die kunnen vinden.

De heer **Six Dijkstra** (NSC):
Ik denk dat we het volledig met elkaar eens zijn. Ik denk dat het goed is dat instanties en bedrijven daar extra op gewezen worden. Ik meen dat de minister daarmee bezig is en dat daar ook handreikingen toe zijn. Maar het is wel lichtelijk absurd om te horen dat er hele advocatenkantoren aan te pas moeten komen voor iets wat mij een heel duidelijke overweging van nationale veiligheid lijkt.

De **voorzitter**:
Dan is het woord aan mevrouw Van der Werf van D66.

Mevrouw **Van der Werf** (D66):
Dank u wel, voorzitter. Dit is mijn eerste debat als nieuwe woordvoerder Digitale Zaken namens D66. Ik heb me in de vorige periode als Kamerlid beziggehouden met veiligheidsvraagstukken, dus ik ben blij dat ik juist in dit debat over onlineveiligheid mijn debuut mag maken in de commissie.

De grootste bedreigingen voor bijvoorbeeld ons bedrijfsleven zijn de bedreigingen online. Daarom heeft de Cyber Security Raad begin dit jaar de formerende partijen opgeroepen om een stap extra te zetten, want de huidige inspanningen en investeringen zijn niet genoeg om Nederland veilig te houden. Dit raakt onze nationale veiligheid en zet onze vrijheid, democratie en welvaart steeds verder onder druk, aldus de raad. Hoe kijkt de minister van EZK naar deze oproep? Is zij het met de raad eens dat, met deze toenemende risico's, die stap extra moet worden gezet? En hoe ziet die er volgens haar uit?

Voorzitter. Op zowel macro- als microniveau staat onze onlineveiligheid onder druk. In het zogeheten Cybersecuritybeeld wordt de volgende conclusie getrokken: de digitale dreiging voor Nederland is onverminderd groot en dat komt onder andere door geopolitieke spanningen. Het is nu een jaar of twee geleden dat de inval door Rusland in Oekraïne plaatsvond. Er zijn een aantal andere geopolitieke spanningen. Ik zal ze niet allemaal noemen, maar die zijn niet gisteren ontstaan. Ik ben benieuwd wat wij zouden kunnen doen om op dat dreigingsniveau te anticiperen en het daadwerkelijk naar beneden te kunnen krijgen.

Voorzitter. Ik vind het ook verrassend dat we weten dat dat dreigingsniveau al een tijdje behoorlijk groot is, maar dat we er bijvoorbeeld niet in slagen om op tijd de Europese cyberveiligheidsrichtlijn hier in te voeren die daar wat aan zou moeten doen. Dan heb ik het over de zogeheten NIS2-richtlijn, die ervoor moet zorgen dat overheidsinstellingen aan de benodigde standaarden voldoen. Dan gaat het over bijvoorbeeld de gemeenten, de Rotterdamse haven en Rijkswaterstaat. Het is cruciaal voor Nederland dat dit soort partijen goed beveiligd zijn. Zonder nationale implementatie kan een toezichthouder daar niet op handhaven, zoals nu natuurlijk ook al het geval is met de Digital Services Act, waarvan we laatst begrepen dat daar op dit moment nog niets mee kan worden gedaan. Die wet is nu naar de Kamer gestuurd, maar we weten dat het weer een tijdje gaat duren voordat we daarmee aan de slag zijn. Ik zou willen voorkomen dat we dat ook bij de NIS2 gaan krijgen, want zonder controle hebben die Europese regels natuurlijk nationaal niet zoveel zin. Hoe kan het dat wij er niet in slagen om die richtlijn op tijd om te zetten? Ik zag ook dat dat in België en Duitsland wel is gelukt en dat het daar al verder op de rit is. Daar zou ik graag een reactie op horen. Is de minister het met mij eens dat we die maatregelen wat meer urgentie zouden moeten geven?

Eerder dit jaar stelde D66 schriftelijke vragen over een groep Chinese hackers die in de mailaccounts van politici en journalisten inbraken. Ook daarvoor geldt: zouden we ons niet beter moeten wapenen tegen dit soort aanvallen, zowel in onze hardware als in onze software?

(vervolg - nieuwe alinea, beurtnummer 4) Mevrouw **Van der Werf** (D66): Voorzitter. Ook op microniveau staat de digitale veiligheid onder druk. 16% van de bevolking is vorig jaar slachtoffer geweest van een onlinemisdrijf; dat is ongeveer een op de zes mensen. 10% van al deze aangiften leidt tot een verdachte. Dat is een heel laag percentage. Er is ook een hele lage pakkans,

dus het is niet verrassend dat cybercrime op dit moment de snelst stijgende vorm van criminaliteit is. Daar hebben we het ook al vaak over gehad in de commissie voor JenV. Cybercrime is een lucratieve business geworden voor criminelen. Onderzoek wijst uit dat er een gebrek aan expertise bij de politie is. Dat is niet zozeer in de cyberteams, maar vooral op het moment dat en de plek waar die aangiften worden gedaan, dus aan de balies. Wat kan de minister van JenV daaraan doen? Ik kan me voorstellen dat dit via iemand anders van het kabinet wordt beantwoord, maar ik vind het wel een belangrijke vraag. Tot nu toe zien we dat die maatregelen te weinig werken, want het afgelopen jaar was er weer een stijging van 20%. Als heel weinig slachtoffers überhaupt aangifte doen en daarvan maar 10% tot een verdachte leidt, dan zijn we echt aan het dweilen met de kraan open. Welke maatregelen neemt het kabinet om het aantal aangiften, de pakkans en ook de expertise omhoog te krijgen?

De Autoriteit Persoonsgegevens sloeg gisteren alarm over de cyberaanvallen, maar bijvoorbeeld ook over de opvolging daarvan. In veel gevallen worden slachtoffers of, als het om bedrijven gaat, klanten van wie gegevens zijn gestolen niet of niet volledig geïnformeerd. Dan kunnen mensen dus ook niet alert zijn op fishingpogingen die via hun verkregen e-mailadres of telefoonnummer worden gedaan. Ik wil als laatste aan de minister het volgende vragen. Wat gaat zij doen om te zorgen dat organisaties die te maken hebben met cyberaanvallen of datalekken hun betrokken klanten informeren, zodat die tijdig alert kunnen zijn en maatregelen kunnen nemen?

Dank, voorzitter.

De **voorzitter**:
Dank u wel. Ik zie geen interrupties. Dan is het woord aan de heer Valize van de PVV.

De heer **Valize** (PVV):
Voorzitter, dank voor het woord. Een aantal onderwerpen zijn al aangestipt, dus ik zal daar kort overheen gaan. Dat spaart mij weer wat tijd uit.

De Rijksinspectie Digitale Infrastructuur maakt zich grote zorgen over een deel van de zonnepaneelomvormers; er is al over gesproken. Die zorg wordt gelukkig gedeeld door iedereen. Er is onderzocht of ze voldoen op het gebied van stoorkans en cyberveiligheid. Er werden een aantal omvormers en een aantal accessoires onderzocht, omdat sommige omvormers niet direct op het

netwerk zitten maar via een accessoire. Vijf van de negen omvormers veroorzaakten storing, geen van de onderzochte omvormers voldeed aan de cyberveiligheid en geen enkel product voldeed aan de administratieve eisen, dus de gebruiksinstructie: hoe moet je ermee omgaan, hoe sluit je 'm aan et cetera.

In de kabinetsreactie lezen we dat het een speerpunt is van het kabinet om in Europa wetgeving hierover vast te stellen. Daar kom ik zo op terug; dat is de Cyber Resilience Act. Het gros van de omvormers komt echter zelden uit Europa. We lezen in het rapport op pagina 38 dat er met alle fabrikanten direct dan wel via hun Europese vestigingen contact is geweest. En dan staat nota bene in het rapport ook nog het verschil uitgelegd tussen het China Export-logo en het Conformité Européenne-logo. Voor velen is dat nauwelijks te onderscheiden, want het lettertype is hetzelfde en het ziet er hetzelfde uit. Het enige verschil is dat er wat meer ruimte tussen de C en de E zit in het geval van het Europese keurmerk. Alsof er buiten Europa niets bestaat. Maar minimaal 71% van de zonnepanelen of de onderdelen daarvan komt uit China. De heer Six Dijkstra stelde daar ook al kritische vragen over, dus daar sluit ik mij graag bij aan. Hoe gaat de minister hierop anticiperen?

Als we kijken naar de Cyber Resilience Act, zien we dat het straks een stap verdergaat. Ze zullen eisen stellen aan de hardware en software van alle producten die een digitale component hebben. Er moet dan gedurende de levensduur van het product, een periode van minimaal vijf jaar, ondersteuning worden geboden in de vorm van beveiligingsupdates. Dat is niet slecht, maar hoe zit het met een product dat de end-of-lifecyclus bereikt en dus een uitfaseertermijn heeft? Hoe zit het daarmee? De CRA heeft ook enkel betrekking op fabrikanten en importeurs in de Europese Unie. Hoe zit het met digitale platforms als Alibaba, AliExpress, SHEIN et cetera, waar consumenten de producten vandaan halen, waaronder ook omvormers en zonnepanelen, die dan vervolgens door een beunhaas op het dak gelegd worden met alle gevolgen van dien?

Voorzitter. Dan kom ik nog even bij het Digital Trust Center. We hebben natuurlijk begrepen dat het traject loopt en we zien ook dat er intensivering is van de samenwerking.

(vervolg - loopt door, beurtnummer 5) De heer **Valize** (PVV):
We hebben de Wet bevordering digitale weerbaarheid bedrijven behandeld. Die is aangenomen, dus dat is al één stap in de goede richting. Verder

worden de drie departementen geïntegreerd tot één apart departement, dat dan onder Justitie en Veiligheid komt te vallen. Dat loopt dus allemaal, maar in ditzelfde stuk wordt ook nog gesproken over de NIS2-richtlijn, waar de collega's het ook al over gehad hebben. Daarin worden de uitkomsten van het rapport voor het herinrichten van het CSIRT-stelsel meegenomen. Wat is hier de status van? We hebben een verzamelbrief ontvangen van de staatssecretaris. Daarin werd vermeld dat deze zou worden omgezet naar Nederlandse wetgeving. Dit komt terug in het notaoverleg van 22 april, dus daar kom ik te zijner tijd nog even op terug. Maar we ontvangen wel signalen dat er wellicht nationale koppen aan toegevoegd gaan worden. In dat kader worden zorgen geuit met betrekking tot de regeldruk. Kan de minister hier al een tipje van de sluier over oplichten? De rest inzake NIS2 nemen we mee naar het notaoverleg.

Voorzitter. Dan hebben we het nog even over de onderzeese datakabels. Ze zijn vitaal verklaard en dat is prima. Ik begreep dat er in september een coördinator is aangesteld voor de zeekabelcoalitie. Worden wij nog nader geïnformeerd over de uitvoering van de coördinerende rol? Het is ook goed dat EZK zal aanhaken op geplande tracés, zowel binnen Europa als continentaal.

Voorzitter. Ik kom bij de voortgang van de Nederlandse Cybersecuritystrategie. Veel trajecten zijn nog in ontwikkeling of zijn nog niet gestart. De wijze van monitoren en evalueren is in ontwikkeling en de nulmeting werd reeds ontvangen, in februari. Dan is de vraag: wat vindt de minister van de aandachtspunten uit het rapport van Dialogic over de beleidslogica van NLCS, zoals over de betrokkenheid van het mkb bij het verbeteren van digitale weerbaarheid en dat er relatief weinig aandacht wordt besteed aan de opschaling van innovaties van producten? Wanneer zullen de resultaten van het aangekondigde onderzoek naar de samenhang tussen AI en cybersecurity naar de Kamer gestuurd worden?

Ten slotte met betrekking tot dit onderwerp. Er wordt aangegeven dat de activiteit bestuurlijk convenant is afgerond en dat die dus niet gemonitord hoeft te worden. Last minute ontvingen wij nog van de Vereniging van Nederlandse Gemeenten de opmerking dat het sluiten van dit convenant slechts een eerste processtap betreft. Zij zouden graag zien dat er wel op gemonitord gaat worden. Kan de minister daar een reactie op geven?

Dan ben ik bij het einde van mijn betoog. Dank u, voorzitter.

De **voorzitter**:
Dank u voor uw bijdrage. Ik vraag de heer Six Dijkstra even of hij de voorzitterstaak kan overnemen, zodat hij mij het woord kan geven.

Voorzitter: Six Dijkstra

De **voorzitter**:
Zeker. Het woord is aan mevrouw Kathmann, van de fractie van GroenLinks-PvdA.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dank u wel, voorzitter. Vandaag werd bekend dat door een softwarelek minstens 26.000 actieve Nederlandse beveiligingssystemen zijn aangetast. Supermarkten, banken, stad- en provinciehuizen, nutsbedrijven, BN'ers, een voormalig minister: allemaal waren ze kwetsbaar. Dienstverleners die hun digitale zaken niet op orde hebben maar wel aan duizenden klanten diensten leveren, zijn het digitale goud voor criminelen. De afnemers zijn de sigaar. Het digitale domein is zo ingewikkeld dat een gemiddelde mkb'er überhaupt niet in staat is om te achterhalen of een alarmsysteem cyberveilig is of niet. Zou de minister kunnen reflecteren op deze casus? Dan bedoel ik een beetje een brede reflectie waarin vragen meegenomen kunnen worden als: moet er voor zo'n geval niet een loket zijn bij het NCSC om die melding beter te kunnen doen? Want er was een melding, maar het was ook een beetje moeilijk om te weten waar je die moet plaatsen als die niet wordt opgevolgd. Kan de minister ook reflecteren op mogelijkheden als boetes die kunnen worden opgelegd?

Die reflectie is belangrijk, omdat we ieder jaar de boodschap krijgen van het Cybersecuritybeeld Nederland dat de digitale dreiging onverminderd groot is. Er gaat geen week voorbij zonder een digitale aanval op een publieke instelling. Het DTC doet oprecht goed werk om ondernemers, van groot tot klein, goed voor te lichten over hoe zij digitaal veilig kunnen worden. Maar uit onderzoek blijkt dat contractuele afspraken over cybersecurity voor ondernemers nauwelijks een rol spelen bij de keuze voor een ICT-product- of dienst.

De tijd is toch wel een beetje voorbij van voorlichten en organisaties zachtjes dirigeren naar cyberveiligheidsmaatregelen.

(vervolg - loopt door, beurtnummer 6) Mevrouw **Kathmann** (GroenLinks-PvdA):
Daarom heb ik de volgende vragen aan de minister. Welke wortel en welke stok gaat ze inzetten om ervoor te zorgen dat het mkb beter aan minimale cyberveiligheidseisen voldoet? Ik zeg dit niet omdat ik mkb'ers regeldruk wil geven of ze wil pesten, maar cybercriminaliteit kost ons miljarden en het kost mkb'ers zelfs de kop. Ik ontvang graag een overzicht van concrete mogelijkheden van maatregelen die verder gaan dan alleen zachtjes dirigeren. Ook vandaag blijkt weer dat veel mensen zich pas bewust worden van cyberrisico's wanneer ze het slachtoffer worden van een hack. Mijn collega van D66 zei het ook al. Dan is het vaak al te laat. Gemiddeld hebben mkb'ers dan tweeëneenhalve ton schade of zijn ze al omgevallen. Kan de minister de mogelijkheid onderzoeken om ethische hackers in opdracht van bijvoorbeeld het DTC in te zetten voor het mkb? Zij kunnen actief op zoek gaan naar kwetsbaarheden bij ICT-leveranciers die grote aantallen mkb'ers treffen. Ik overweeg een motie hierover in te dienen, ook omdat het een mooi gebaar zou zijn richting het mkb.

Voorzitter. Verder moeten we één ding niet vergeten: geen enkele firewall kan op tegen een menselijke fout en fouten maken is nu eenmaal menselijk. Mensen blijven de zwakste schakel in cybersecurity. Tegelijkertijd is educatie van gebruikers om zich beter te beveiligen maar tot zover een oplossing. Naast cybersecurity zijn er namelijk nog duizenden dingen waarvan mensen geacht worden het te snappen. Hoe fijn zou het zijn als je als gebruiker ervan uit kan gaan dat je apparaat of dienst sowieso al veilig is en dat dat ook de hele levensduur zo blijft? Is de minister bereid te kijken naar mogelijkheden om informatie over de cyberveiligheid en het updatebeleid van diensten en apparaten verplicht kenbaar te maken aan consumenten? Consumenten kunnen zo een geïnformeerd besluit nemen over hun aankoop. Is de minister bereid om in Europa aan te dringen op hogere standaarden wat betreft de cybersecurity van diensten en apparaten, security by design en cyberveiligheid voor de gehele levensduur van het apparaat? Welke mogelijkheden ziet de minister op dit gebied?

Voorzitter. Daarnaast heeft iedereen recht op veiligheid, maar in het digitale domein lijkt dat niet op te gaan. Cyberveiligheid is geprivatiseerd. Bij Meta en andere websites moet je betalen voor je privacy. Wachtwoordmanagers, VPN's, antivirus, het kost allemaal geld. Dure telefoons zijn beter beschermd dan goedkope toestellen. Als je minder te besteden hebt, ben je dus minder veilig. Daarom wil ik nog de volgende vragen stellen. Vindt de minister dat

free and open-source software die een bijdrage levert aan de cybersecurity van mensen actief moet worden aangeboden of aanbevolen door de overheid? Hoe kan zij deze software voor iedereen vindbaar en begrijpelijk maken? Is de minister bereid om te kijken naar mogelijkheden waarbij bijvoorbeeld bibliotheekmedewerkers of gemeenten ondersteuning kunnen bieden aan mensen met een klein budget bij het cyberveilig houden van hun apparaten en diensten?

Ten slotte, de laatste vraag. In het rapport over de nulmeting van de Nederlandse Cybersecuritystrategie wordt duidelijk stilgestaan bij het probleem van het tekort aan cybersecurityspecialisten op de arbeidsmarkt. Dat tekort neemt alleen maar toe. Waar komt dat tekort volgens de minister vandaan en hoe gaat het kabinet dit oplossen? Kan zij ook een concreet actieplan maken voor meer vrouwen in de cybersecuritysector? Gisteren zag ik een ongelofelijk mooie poster waar "geen Cinderella's maar Cyberella's" op stond.

De **voorzitter**:
Dank u wel. Ik draag het voorzittersstokje weer over aan mevrouw Kathmann.

Voorzitter: Kathmann

De **voorzitter**:
Dank u wel. Ik kijk even naar de minister. We schorsen twintig minuten. Daarna gaan we door met de beantwoording van de minister.

De vergadering wordt van 13.28 uur tot 13.57 uur geschorst.

De **voorzitter**:
We gaan verder met het debat over cybersecurity en veiligheid. We gaan naar de minister voor de beantwoording.

Minister **Adriaansens**:
Dank u, voorzitter. Ik heb een paar hele korte inleidende woorden. Daarna zal ik snel overgaan tot de vraagbeantwoording. We spreken vandaag over onlineveiligheid en cybersecurity. Op 12 maart hebben een groot deel van uw commissie en ik elkaar ook gesproken over de behandeling van het wetsvoorstel Bevordering digitale weerbaarheid bedrijven. Met een ruime

meerderheid heeft u voor dat wetsvoorstel gestemd. Daar wil ik u voor bedanken, want daarmee kunnen wij dus weer stappen zetten.

Vandaag staan er weer een aantal belangrijke punten op de agenda. We constateren eigenlijk allemaal dat de digitale dreiging nog steeds onverminderd hoog is. Dat heeft u ook kunnen lezen in het laatste Cybersecuritybeeld Nederland. Daarom zijn we hard bezig met de implementatie van de Nederlandse Cybersecuritystrategie. Het cybersecuritystelsel in Nederland is volop in beweging om de kloof tussen de digitale dreiging en het bevorderen van de weerbaarheid te verkleinen, bijvoorbeeld door de integratie van het Nationaal Cyber Security Centrum, het Digital Trust Center en het Computer Incidents Response Team. We moeten nog steeds eens zoeken naar de Nederlandse woorden hiervoor, maar we begrijpen volgens mij allemaal wat ermee bedoeld wordt. We zijn ook bezig met de implementatie van de NIS2, de herziene Netwerk- en informatiebeveiligingsrichtlijn.

Daarnaast zal de minister van Justitie en Veiligheid u op korte termijn informeren over de stappen die we zetten om de publiek-private samenwerking te verbeteren via de doorontwikkeling van het landelijk dekkende stelsel van cybersecuritysamenwerkingsverbanden. Die kunt u overigens vinden op de website van het DTC.

Ook wil ik ondernemers helpen bij het kiezen van een betrouwbare ICT-leverancier, met behulp van een keurmerk. We hebben de cyberoefening die ondernemers zelf kunnen uitvoeren, ook op de website van het Digital Trust Center gelanceerd. Die kan je ook daar vinden. Op deze manier kunnen ondernemers in de praktijk ervaren en oefenen hoe ze zich het best tegen een cyberaanval kunnen beschermen.

Voorzitter. We spreken vandaag ook over veilige digitale producten en diensten. Europese maatregelen, zoals wetgeving en certificering, zijn hard nodig om de leveranciers en fabrikanten meer verantwoordelijk te maken voor de veiligheid van hun product en dienst. Denk bijvoorbeeld aan het veiliger maken van de zonnepanelen. Dat is hier ook benoemd. We willen natuurlijk voorkomen dat een groot aantal apparaten op afstand gelijktijdig zou kunnen worden gehackt. Met het Europese akkoord op de Cyber Resilience Act hebben we daarvoor een belangrijke mijlpaal bereikt. Nu gaat onze volle aandacht uit naar de implementatie daarvan.

We hebben het vandaag ook over de vitaalbeoordeling van onderzeese datakabels, de zeekabels. Die heeft vorig jaar plaatsgevonden. Er wordt nu heel hard gewerkt aan het vaststellen welke aanbieders binnen die zeekabelinfrastructuur vitaal moeten worden.

Voorzitter. Ten slotte doe ik, mede namens de minister van JenV, het aanbod aan deze commissie om op werkbezoek te gaan bij het Nationaal Cyber Security Centrum en het Digital Trust Center. Zij zouden u heel graag ontvangen om te laten zien wat zij allemaal doen.

Ik zal nu ingaan op de vragen. Als u mij toestaat, voorzitter, heb ik daarvoor vier mapjes. Ik wil er ook wel vijf van maken, maar vier leek mij wel voldoende voor vandaag. Het eerste gaat over pijler I van de cybersecuritystrategie, de digitale weerbaarheid. Ik heb ze naar de pijlers geordend. Het tweede gaat dus over pijler II van de cybersecuritystrategie. Dat gaat over de veilige digitale producten en diensten. Het derde betreft de derde pijler en gaat over het tegengaan van de digitale dreigingen. Het vierde gaat natuurlijk over pijler IV van de cybersecuritystrategie, over de arbeidsmarkt, het onderwijs en de digitale weerbaarheid van burgers. Dan heb ik nog een mapje overig.

Allereerst pijler I. Mevrouw Rajkowski vroeg naar het beeld. Ze zegt dat het gevraagd en ongevraagd informeren nog te weinig gebeurt buiten die vitale infrastructuur. Wat is er nodig om de dienstverlening van het Digital Trust Center rondom gevraagd en ongevraagd notificeren snel uit te breiden? Ik ben het volledig met haar eens dat er altijd winst te behalen valt, maar de ongevraagde dienstverlening van het Digital Trust Center is sinds 2021 flink uitgebreid en wordt ook nog verder ontwikkeld. Het Digital Trust Center verstuurt dagelijks ongevraagd informatie over cyberdreigingen naar individuele bedrijven. Er wordt ook heel erg nauw samengewerkt met het Nationaal Cyber Security Centrum aan een portal, een portaal, waar bedrijven op kunnen aansluiten. Door middel van dat portaal kunnen bedrijven gerichter geïnformeerd worden over alle cyberdreigingen die voor hen relevant zijn. De verwachting is dat voor de zomer van dit jaar de eerste bedrijven die deel uitmaken van de pilot van het DTC, ook aangesloten kunnen worden op dat portaal.

(vervolg - loopt door, beurtnummer 8) Minister **Adriaansens**:
En het streven is dan om eind 2024 alle 50 pilotdeelnemers op die manier te bedienen. We hopen dat daarna ook verder uit te breiden.

De heer Six Dijkstra vroeg of we niet moeten afstappen van een landenneutrale aanpak, aangezien iedereen weet waar de dreiging vandaan komt. Dat doen we niet op die manier; het aanpakken van nationale veiligheidsrisico's als gevolg van statelijke dreigingen luistert namelijk heel erg nauw. Het vereist maatregelen die gericht zijn, die proportioneel zijn, die adaptief zijn, maar die vooral ook risicogebaseerd zijn. We hebben namelijk een aanpak nodig die toepasbaar is op dreigingen vanuit elke statelijke actor, en dat is geen statisch gegeven, helaas. We kunnen gerichte maatregelen nemen daar waar dat nodig is. De instrumenten binnen die landenneutrale aanpak spitsen we dan toe op de landenspecifieke risico's. Wat nou precies die dreigingen en risico's zijn, staat in het Dreigingsbeeld statelijke actoren. En ook het proactief handelen van de diensten, laat ik dat niet onvermeld laten. Die zijn zeer actief. Individuele bedrijven en publieke instellingen worden ook geïnformeerd over die dreigingen. Dus niet een landenspecifieke aanpak, maar wel een hele serieuze, gerichte aanpak.

De **voorzitter**:
U heeft een interruptie van de heer Six Dijkstra, NSC.

De heer **Six Dijkstra** (NSC):
Ja, dank u wel, voorzitter. En ook dank aan de minister. Ik weet niet of de minister er nog op terugkomt, maar mijn vraag zag natuurlijk specifiek op een landengerichte aanpak als het gaat om juist de apparaten die met het internet verbonden zijn, dus de routers, de switchers en de edge-apparatuur, aangezien het welbekend is dat het een modus operandi van China is dat zij in dat soort apparaten backdoors kunnen bouwen, dat ze die kunnen hacken. Dus voor dat specifieke onderdeel. Is daar niet nog van af te stappen, van die landenneutrale aanpak? Hoe kijkt de minister daartegen aan?

Minister **Adriaansens**:
Ik weet dit niet specifiek en zal het nog even checken, maar in algemene zin gaan we natuurlijk naar Europese regelgeving toe die alle beveiliging op het gebied van cyber in 2025 gaat regelen. Dus we moeten heel goed opletten op wat specifiek is en wat algemeen. Waar wij heel erg voor pleiten, is een algemene regeling, waarbij fabrikanten gedwongen worden om rekening te houden met de cybersecurityeisen. Ik zal dat zo dadelijk wat toelichten, maar het gaat bijvoorbeeld ook over security by design. Daarmee zou je al een heleboel kunnen afvangen. We willen ook een open handelsland zijn; we willen niet barrières waar dat niet nodig is, we zullen heel gericht moeten zijn. Maar in algemene zin geldt voor alle producten die we dadelijk in de

markt gaan gebruiken die digitaal zijn of via het internet verbonden zijn, dat daar cybersecurityeisen aan moeten worden gesteld. Dan vang je echt al heel veel af.

Voorzitter. De heer Six Dijkstra vroeg ook of de ABRO-regeling nog iets gaat veranderen om die statelijke actoren buiten de deur te houden. Dat "ABRO" is de Algemene Beveiligingseisen Rijksoverheid Opdrachten. Het beoogt de inkoopeisen voor en toezicht op veiligheidsgerelateerde overheidsorganisaties te beschrijven. Op basis daarvan zullen voor de nationale veiligheid dus beperkingen gelden voor landen met een actief cyberprogramma gericht tegen Nederland. Er wordt nog onderzocht of daar thans een wettelijk kader voor bestaat of dat we daar een nieuw kader voor moeten invoeren.

D66 vroeg wat ik vind van de oproep van de Cyber Security Raad aan het nieuwe kabinet om sterk in te zetten op cybersecurity. In algemene zin ben ik het daar eigenlijk volmondig mee eens, want dat kan niet genoeg zijn, gezien ook de omvang van de dreigingen die wij zien. Desalniettemin meen ik ook dat wij al best flink geïnvesteerd hebben in een aanpak, alleen kost het tijd om het volledig te implementeren. We hebben dus een nationale cybersecuritystrategie, en die voeren wij uit. We hebben ook extra middelen voor het tegengaan van digitale dreigingen door statelijke actoren en criminelen, en om daar acties op te zetten. Dat vindt u allemaal terug in die Nederlandse cybersecuritystrategie. Daar gaan we ook onverminderd mee door. En wat een volgend kabinet doet ... Ik kan het alleen maar van harte aanbevelen, want dit wil volgens mij iedereen. Er is volgens mij niet zo veel verschil in de Kamer over hoe belangrijk het is om dit aan te pakken.

Voorzitter. De heer Six Dijkstra en mevrouw Van der Werf vroegen waarom de implementatie van die NIS2-richtlijn zo lang duurt. Ik ben het daar eigenlijk, als je er oppervlakkig naar kijkt, ook wel mee eens: goh, wat kost dat nou veel tijd. Maar het is wel een heel complex traject.

(vervolg - loopt door, beurtnummer 9) Minister **Adriaansens**:
Want wat wij willen doen ... We hebben een heleboel zaken sectoraal geregeld, en willen het ook toespitsen op bijvoorbeeld de zorg of het watermanagement, zodat we zorgen dat we de bedrijven en organisaties die daarin actief zijn daadwerkelijk de goede keuzes laten maken. Deze richtlijnen zullen aangrijpende gevolgen hebben voor duizenden organisaties. Dat geldt voor de entiteiten die aan de verplichtingen moeten voldoen, maar

ook voor de departementen, de uitvoeringsorganisaties en de toezichthouders, die nieuwe taken krijgen, waarvoor ze uitgerust moeten zijn. Eigenlijk herzien we met deze wet het volledige cybersecuritystelsel in Nederland. Voorbeelden daarvan zijn samenwerkingsafspraken tussen het NCSC en DTC -- doe mij nog maar een afkorting ... -- en de zorgsector, en ook bijvoorbeeld het delen van dreigingsinformatie: hoe deel je die informatie goed? Maar bijvoorbeeld ook het toezicht organiseren op de voedselvoorziening, het opzetten van een centraal portaal. Dat is de reden dat dit tijd kost.

De heer **Six Dijkstra** (NSC):
Maar dan was toch mijn vraag aan de minister, en misschien gaat mijn buurvrouw dezelfde vraag stellen: hoe komt het dan dat het andere landen wel lukt, als het dezelfde wetgeving is?

Minister **Adriaansens**:
Dat is een goede vraag. Andere landen hebben soms een algemene regel. Wij spitsen het toe op de sectoren, waardoor het meer tijd kost maar hopelijk ook effectiever gaat zijn.

Mevrouw **Van der Werf** (D66):
Er is natuurlijk jarenlang onderhandeld over deze richtlijn. Toen had Nederland ook al kunnen bedenken, als het antwoord is dat wij het meer toespitsen, dat we daar dan tijd en dus ook capaciteit voor nodig hebben. Dus ik vind dat wel een beetje een makkelijk antwoord, zeg ik in alle eerlijkheid. We hebben heel lang onderhandeld over al die regels en richtlijnen, en vervolgens regelen wij het toezicht niet. Dus maakte de minister zich niet boos toen zij hierachter kwam, of dacht zij van begin af aan al dat wij daar gewoon wat langer over zouden doen? Ik snap het niet helemaal. Bij de DSA zagen we dat ook gebeuren, en nu worden we weer ingehaald. Ik zou willen voorkomen dat wij straks de enigen in Europa zijn waar er regels op papier zijn waar in de praktijk niet zo veel mee gebeurt.

Minister **Adriaansens**:
Dat is volgens mij niet het correcte beeld. Ik begrijp wel dat deze vraag gesteld wordt. Als je bijvoorbeeld naar Duitsland kijkt, dan maken ze daar wel een generieke regel, maar die moet nog wel door de Länder worden ingevoerd. Dus de vraag is wanneer het daar ook daadwerkelijk tot implementatie leidt. Wat wij hier hebben, is een best wel ver doorgevoerde sectorale opbouw van regels, toezichthouders, in de zorg, op het gebied van

allerlei infrastructuur. Wij moeten zorgen dat wij dat allemaal op elkaar laten aansluiten. Daarom kost het nu meer tijd, maar we hebben wel de verwachting dat het aansluit bij zoals wij gewend zijn te werken, maar ook dat we veel gerichter actie kunnen ondernemen als het daadwerkelijk geïmplementeerd is. Ik wil wel gezegd hebben dat ik het op papier ook een lange tijd vind. Ik bedoel, daar hebben we volgens mij geen discussie over. Maar gezien het beeld dat ik aangereikt krijg en de informatie daarover, begrijp ik wel waarom het zo lang duurt.

Mevrouw **Van der Werf** (D66):
Dan ga ik proberen om twee vragen in één vraag te stoppen, voorzitter, want u bent streng. Ik zou heel graag willen weten van de minister wat dan de tijdlijn is die zij voor zich ziet om die NIS2-richtlijn om te zetten in nationale regelgeving, want ik ben dan ook wel benieuwd wanneer we dat wél kunnen verwachten, en of je ergens onderweg in die tijdlijn toch wel zou kunnen zeggen ... Want ik begrijp haar antwoord wel, dat het belangrijk is dat die sectoren op elkaar aangesloten zijn, maar wat bij die DSA vooral jammer is, is dat het toezicht nog niet functioneert. Dus zou je al onderweg kunnen zeggen: we beginnen wel deels met handhaven en wachten niet tot het complete kaartje aan elkaar is genaaid -- om het zo maar te zeggen?

Minister **Adriaansens**:
Het toezicht zal hier niet het heikele punt zijn, omdat we dus zorgen dat de bestaande toezichthouders deze implementatie voor hun rekening gaan nemen. Dat is dus al ingeregeld. We wachten even met het tijdpad totdat de minister van JenV de conceptvoorstellen voor deze zomer naar uw Kamer stuurt. Dat is op zich een overzienbare periode. Maar we gaan ondertussen wel beginnen. Dus wij zijn al bezig om daar waar er nog geen verplichting is, organisaties wel voor te bereiden op de taak die komt. En ik voeg daar nog aan toe dat half mei de consultatie start.

Mevrouw **Van der Werf** (D66):
Dat had ik ook gezien. Tegelijkertijd zou ik heel graag zien dat we die deadline halen. Ik meen dat die in oktober ligt of dat die in het najaar is. Je zou namelijk kunnen zeggen: als die consultatie in het voorjaar start, dan kan je input daarvan in de zomer verwerken. Volgens mij kan je dan nog wel in een paar maanden een inhaalslag maken.

Minister **Adriaansens**:
Dat ligt voor een deel buiten mijn invloedssfeer. Het gaat naar de Kamer.

Daarna moet het naar de Raad van State. Je hebt dus eerst de consultatie, dan de Kamer, dan de Raad van State en dan het parlementaire behandelingsproces. Voor een deel ligt dat, als ik voorzichtig ben, aan de andere kant van de tafel. Wij zullen zorgen dat we het zo snel mogelijk voor de zomer aanbieden.

Voorzitter. De heer Valize vroeg met het oog op de NIS2 of er een herinrichting van het CSIRT, van het stelsel is aangekondigd en wat de status is. Naar verwachting zullen we de NIS2-richtlijn dit najaar aan de Kamer zenden, in de hoop dat we daar dan doorheen zijn. Zo zie je, twee ministeries hebben een iets andere taal over de planning, maar we bedoelen hetzelfde. De uitwerking van dat CSIRT-rapport wordt parallel daaraan uitgevoerd. Daarover wordt u dus gelijktijdig geïnformeerd. De uitwerking van het rapport is erop gericht om organisaties te ondersteunen in het beter beveiligen van de systemen, te informeren over de bekende kwetsbaarheden en bedreigingen, en bijstand te verlenen in het geval van een incident.

De heer Valize vroeg ook of ik iets kon zeggen over de gevolgen voor de regeldruk die daaruit voortkomt. Zoals ik al zei, zitten we in de laatste fase van de voorbereiding. Hoe het er dan precies uitziet, kan ik nog niet zeggen. Maar het is wel duidelijk dat de richtlijn eisen met zich meebrengt voor nieuwe organisaties. Dat is ook nodig voor de digitale weerbaarheid van Europa en Nederland. Zoals ik net al aangaf, communiceren wij nu al, zodat zij zich kunnen voorbereiden. Bij het opstellen van die regelgeving hebben we natuurlijk wel oog voor de regeldruk. Wij proberen ook altijd contact te hebben met organisaties, te reflecteren en te kijken hoe we een bepaald doel kunnen bereiken met de minste regeldruk.

Volgens mij vroeg de PVV, de heer Valize, ook waarom het bestuurlijk convenant digitale veiligheid niet wordt meegenomen in de monitoring. Het wordt wel meegenomen. Het is onderdeel van het actieplan Nederlandse Cybersecuritystrategie. Op dit moment zijn de projectleiders van het Rijk en de Vereniging van Nederlandse Gemeenten samen bezig met formuleren van de acties die daaruit voortkomen. We hebben een structuur ingericht voor de monitoring op die acties. Het wordt dus niet afzonderlijk meegenomen, maar het zit in het totaal. Het loopt mee als onderdeel van de Cybersecuritystrategie en de rapportages die we daarover doen aan uw Kamer.

Mevrouw Van der Werf van D66 vroeg wat we doen om de aangiftebereidheid en de pakkans te vergroten. Ik wil zeker, mede namens de minister van JenV, de slachtoffers vooral oproepen om aangifte te doen bij de politie. Meer aangiftes leiden ertoe dat het totaalbeeld van het probleem beter wordt. Dat bevordert dus ook de aanpak en het treffen van maatregelen. Een van de acties uit de Nederlandse Cybersecuritystrategie is het voor meer cybercrimefenomenen mogelijk maken om online melding of aangifte te doen. Over de voortgang van die actie rapporteren we in de voortgangsrapportage Nederlandse Cybersecuritystrategie. Dat doen we in het najaar van 2024.

Voorzitter. Mevrouw Kathmann vroeg of ik de mogelijkheid wil onderzoeken om ethische hackers bij het DTC in te zetten om digitale kwetsbaarheden te onderzoeken. Het Digital Trust Center en het Nationaal Cyber Security Centrum werken al samen met ethische hackers, bijvoorbeeld met het DIVD. Samen wisselen zij informatie uit over die kwetsbaarheden. We kunnen wel kijken naar intensivering daarvan, maar ik weet dat er al veel gebeurt. Verder zullen we in het programma Cyclotron samenwerken om die dreigingsinformatie nog beter te analyseren.

Voorzitter. Dan een vraag van de PVV over de nulmeting van de NLCS, de Nederlandse Cybersecuritystrategie, namelijk wat ik vind van de aandachtspunten bij beleidslogica, zoals betrokkenheid van het mkb. Ik ben het helemaal eens met de PVV dat het belangrijk is en dat het WODC hele belangrijke aanbevelingen en analyses doet in het omvangrijke rapport.

(vervolg - loopt door, beurtnummer 11) Minister **Adriaansens**:
Wij gaan er ook mee aan de slag, voor zover wij daar niet al mee aan de slag zijn.

Ik wil allereerst een aantal zaken benoemen. Ik zal daarin niet volledig zijn, want we doen echt heel veel. De minister van Justitie en Veiligheid is met collega's in gesprek over hoe de conclusies kunnen worden meegenomen in de uitvoering van de cybersecuritystrategie. Ze zal datgene wat daaruit komt, meenemen boven op datgene wat we al doen in de voortgangsrapportage. U heeft de Wet bevordering digitale weerbaarheid bedrijven aangenomen, waarmee ik nog meer aan voorlichting kan doen en waarmee ik nog meer acties kan nemen richting bedrijven. Ik kan ook meer doen met informatiedeling et cetera et cetera. Als je naar de website van het DTC gaat, dan zie je ook dat er allerlei tools beschikbaar zijn. Mevrouw

Rajkowski is inmiddels weer terug. De cybersecurityoefening is geïmplementeerd. Die kun je ook terugvinden op de website, net als het keurmerk. Op die manier proberen we de betrokkenheid van het mkb te vergroten.

Voorzitter. Ik kom op de vraag over datalekken. Ik zit even te kijken van wie die vraag ook alweer was. Wat gaat de minister doen om ervoor te zorgen dat organisaties hun klanten informeren die betrokken zijn bij een incident? Die vraag was van D66. Het is zorgelijk dat organisaties niet altijd hun klanten informeren. Het zou ons ontzettend helpen als zij dat wel doen, want dan zijn we allemaal weer een stukje veiliger. Op grond van de AVG moet een bedrijf dat een datalek heeft geconstateerd, dat binnen 72 uur melden aan de Autoriteit Persoonsgegevens. De slachtoffers moeten ook worden geïnformeerd als het datalek voor hen waarschijnlijk een groot risico oplevert. Het kabinet heeft extra middelen vrijgemaakt voor de Autoriteit Persoonsgegevens om ervoor te zorgen dat zij haar taken nog beter kan uitvoeren. De AP houdt toezicht op de naleving van de AVG en kijkt ook of het slachtoffer wordt geïnformeerd als er sprake is van een datalek.

Voorzitter, dat waren mijn antwoorden op de vragen in het eerste blokje.

Ik ga ongemerkt door naar blokje twee, over pijler II van de Cybersecuritystrategie. Mevrouw Rajkowski vroeg naar de omvormers. Daar heeft de RDI voor gewaarschuwd. Dat is inderdaad een zorg. De RDI heeft gewaarschuwd voor het op afstand aan- en uit kunnen zetten van zonnepaneelinstallaties via gehackte omvormers. Daarmee ontstaat een risico op misbruik. Dat kan best een grote impact hebben, bijvoorbeeld als het hele elektriciteitsnetwerk uit zou vallen. De aankomende cybersecurityeisen op grond van de Radio Equipment Directive bepalen dat omvormers moeten worden beveiligd tegen onbevoegde toegang. We hebben dus wel perspectief op een regeling. Helaas duurt de uitwerking van de cybersecuritystandaarden van de RED wat langer, waardoor de Europese Commissie de ingangsdatum met een jaar heeft uitgesteld. Die is nu augustus 2025. U noemde 2024, maar het is 2025.

Wij roepen in de tussentijd wel alle fabrikanten op om de beveiliging op peil te brengen. De RDI is zich ook aan het voorbereiden op haar toezichtsrol. Het helpt bijvoorbeeld enorm als consumenten en bedrijven de standaardwachtwoorden van de omvormers wijzigen in een sterk wachtwoord. Er ligt dus ook een voorlichtingsrol bij de overheid om te

zeggen: doe je updates. Maar het is breder dan dat. We moeten niet alleen maar roepen: doe je updates. We moeten daar echt veel meer aandacht aan besteden, want dat helpt enorm.

Mevrouw **Rajkowski** (VVD):
Dit is natuurlijk lastig; dat begrijp ik. Als de veiligheidseisen pas in 2025 ingaan, dan is het natuurlijk lastig om nu te handhaven en te beboeten. Tegelijkertijd zou je toch heel graag wat willen doen. Is het mogelijk om de randen wat op te zoeken? Het is goed dat er gesprekken worden gevoerd met fabrikanten. Ik kan me voorstellen dat de een wat welwillender zal zijn en beter zal luisteren dan de ander. Stel dat fabrikanten nu al worden gewaarschuwd maar straks, vanaf die datum, niet aan de juiste eisen voldoen. Kunnen ze dan meteen worden beboet in plaats van dat ze eerst een waarschuwing krijgen? Dan kunnen we misschien wat dwingender de juiste kant op duwen, want anders moeten we anderhalf jaar wachten en dat is best wel lang.

Minister **Adriaansens**:
Ik ben het ermee eens dat dat best lang is. Ik wil gaan kijken wat ik kan doen met het DTC. Daar kom ik dan heel graag op terug. We doen een najaarsvoortgangsrapportage. Ik zal bekijken wat we kunnen doen wat betreft het anticiperen op die regelgeving.

Voorzitter. Dan de vraag van de PvdA over de bereidheid om binnen Europa aan te dringen op hogere standaarden wat betreft de cybersecurity van diensten en apparaten, over security by design. Zoals gezegd deel ik het belang daarvan. Daarom is het ook een doelstelling binnen de Nederlandse Cybersecuritystrategie. Wij hebben als Nederland bij de Europese Commissie heel erg aangedrongen op die algemene eisen voor alle digitale producten die in de Europese Unie op de markt komen. We zijn daarmee al begonnen voordat de Commissie het voorstel deed voor de Cyber Resilience Act. Ook tijdens de onderhandelingen hebben we daar met een hoog ambitieniveau flink wat invloed op uitgeoefend. Het resultaat mag er naar ons idee zijn: alle digitale producten inclusief hardware, software en losse componenten in de hele toeleveringsketen moeten vanaf 2027 passend beveiligd zijn. Daarbij geldt dat security by design een vereiste is en dat producten zonder bekende kwetsbaarheden op de markt moeten worden gebracht. Ze moeten er dus mee aan de slag. Fabrikanten blijven gedurende de hele verwachte gebruiksduur verplicht om kwetsbaarheden op te lossen door gratis veiligheidsupdates te verstrekken.

Voorzitter. Een van uw leden had het nog over end-of-life. Dat is dan ook echt end-of-life. Als een product nog functioneert, moet dat aan de eisen voldoen. Is dat niet meer zo, dan mag je dat ook niet meer op de markt hebben, want anders zou je een product nog kunnen blijven verkopen terwijl dat niet meer aan de standaarden voldoet.

De heer **Valize** (PVV):
Met de end-of-lifecyclus bedoelde ik meer de uitfaseerperiode. Voordat een voorraad weg is, gaat er nog wat tijd overheen. Is daar ook over nagedacht?

Minister **Adriaansens**:
Sorry, ik was even afgeleid.

De heer **Valize** (PVV):
Aan het eind van die end-of-lifecyclus heb je nog altijd voorraad. Die voorraad moet ook uitverkocht, dus je hebt een uitfaseerperiode. Is daar ook over nagedacht?

Minister **Adriaansens**:
Dat is een goede vraag. Daar had ik ook even ruggespraak over. Uiteindelijk moet de eigenaar de handeling verrichten. Die moet de voorraad terugnemen. RDI moet daar toezicht op houden. Dat is de wijze waarop het geregeld is. Maar we moeten er heel erg alert op zijn, want daarmee zou je het hele systeem kunnen ondergraven en dat is niet de bedoeling. In die verantwoordelijkheidsverdeling wordt het dus geregeld. Ik krijg nu toegefluisterd dat de fabrikant moet melden wat de beëindigingsdatum is van de ondersteuning. Dan heeft u meer informatie.

De **voorzitter**:
U heeft nog een interruptie van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):
Tijdens de eerste termijn is de casus van de kwetsbare alarmsystemen al benoemd. Die casus was vandaag in het nieuws. Mijn vraag aan de minister is: wat voor effect zou het hebben gehad op deze casus als de Cyber Resilience Act in werking was getreden?

Minister **Adriaansens**:
Dan had je aan de voorkant hogere eisen gesteld aan die software. Maar ik twijfel even, want ik kan niet beoordelen wat het risico … Kijk, aan de

voorkant haal je een heleboel risico's weg omdat een product aan de door ons gestelde cybersecurityeisen moet voldoen. Voldoet dat daar niet aan, dan kun je zelfs een boete krijgen et cetera. Daar wordt hard op gehandhaafd. Maar er kan natuurlijk een risico zijn dat je erdoorheen gaat, wat dan weer leidt tot een aanscherping van eisen. Volgens mij moeten we met elkaar zo'n systeem gaan organiseren. Ik kan over deze casus dus niet zeggen dat het anders niet was gebeurd, maar ik weet wel dat het risico kleiner was geweest.

De **voorzitter**:
U heeft nog een interruptie van de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
In deze casus was het bij de fabrikant al een jaar bekend dat de kwetsbaarheid erin zat. Een klokkenluider had dat aan de fabrikant gemeld en daar is vervolgens niet op geacteerd. Wat zouden onder de CRA de gevolgen daarvan zijn?

Minister **Adriaansens**:
Dat is precies de crux. Bij een bekende kwetsbaarheid had de fabrikant dit moeten oplossen. De aangescherpte eisen schelen dus wel. Dan had er ook een boete boven het hoofd van de fabrikant gehangen.

(vervolg - nieuwe alinea, beurtnummer 13) Minister **Adriaansens**:
Voorzitter. De PVV vroeg hoe de minister gaat anticiperen op de cybersecurityeisen ten aanzien van de Europese wetgeving. Volgens mij heb ik al aangegeven dat de RED per 1 augustus 2025 ingaat en dat we daar dus op anticiperen. Ik heb ook al gezegd dat we daar proactief in zijn.

Mevrouw Kathmann, PvdA, vroeg naar betere informatievoorziening aan consumenten over het niveau van de beveiliging van de apparaten en diensten die ze aanschaffen, een soort veiligheidslabel. Juist consumenten zouden erop moeten kunnen rekenen dat een apparaat dat in de Europese Unie wordt aangeboden veilig is. Dat geldt al voor fysieke veiligheid. Denk aan geen kankerverwekkende stoffen en geen brandgevaar, maar het moet dus ook voor cybersecurity gaan gelden. Een label laat de verantwoordelijkheid voor de juiste keuze bij de consument. In plaats daarvan heb ik me hardgemaakt voor verplichte cybersecurityeisen voor alle hard- en softwareproducten die in Europa op de markt komen. Fabrikanten mogen met de komst van de Cyber Resilience Act -- die komt er zoals gezegd

vanaf 2027 -- alleen nog maar digitale producten op de markt brengen die digitaal veilig zijn. Dat niveau van beveiliging moet passend zijn met het oog op de risico's die bij het product horen. Fabrikanten moeten de producten na verkoop ook veilig houden voor de hele verwachte gebruiksduur. De Cyber Resilience Act verplicht tot het bij de aanschaf duidelijk vermelden van deze ondersteuningstermijn en de CE-markering. Dat is dus het label. De Cyber Resilience Act, de CRA, gaat voor alle hard- en software en losse componenten gelden, zowel voor consumentenproducten als voor zakelijk gebruik en industriële toepassingen. Eigenlijk stellen we met de Radio Equipment Directive vanaf 2025 al de eerste eisen voor draadloos verbonden apparaten.

Deze vraag van mevrouw Kathmann, GroenLinks-PvdA, hoorde misschien in het eerste mapje thuis, namelijk: welke mogelijkheid is er om die cyberveiligheidseisen op te stellen voor het midden- en kleinbedrijf met een zo klein mogelijke toename van de regeldruk? We waren net al een beetje in gesprek over wat we doen om het mkb te ondersteunen. Dit is de andere kant van de medaille. Die digitale veiligheid is echt een voorwaarde, ook voor dit soort bedrijven. Ze moeten hun basis op orde hebben. Ik ben alleen niet voor het opstellen van extra eisen, omdat dat niet echt doenlijk is. De diversiteit onder de bedrijven is echt heel groot. Het mkb is een hele brede verzameling van soorten bedrijven. In de praktijk zorgt ook heel vaak de IT-dienstverlener voor de cybersecurity. Die eisen moeten wel proportioneel zijn voor de betreffende bedrijven. Maar goed, met de NIS2 gaan we echt al een heel grote stap zetten. We doen dus al het nodige, maar dat hoef ik mevrouw Kathmann niet uit te leggen; die weet dat heel goed. Bedrijven, ook mkb'ers, moeten meer weerbaar worden en ook eisen gaan stellen aan hun toeleveranciers. Ik denk dat dat heel belangrijk is. Voor een deel worden ze daar ook in gefaciliteerd door het Digital Trust Center, onder andere met de CyberVeilig Check, die daar te vinden is. Daarmee kan je goed kijken welke acties je moet ondernemen, ook als je zelf wat minder kennis in huis hebt.

De PVV vroeg naar digitale platformen als AliExpress. De eisen van de CRA gelden ook voor geïmporteerde producten van buiten de Europese Unie. Importeurs zijn verplicht om bij de fabrikant na te gaan of de producten voldoen aan de eisen. De RDI gaat daar dan ook toezicht op houden. Als een importeur het vermoeden heeft dat een product niet voldoet, dan moet de importeur dat verplicht melden bij de toezichthouder.

De heer **Valize** (PVV):
Mijn vraag ging eigenlijk meer over consumenten. Wat als consumenten het zelf bestellen via AliExpress of een van die andere platformen en het door een beunhaas wordt geïnstalleerd op de daken? Daar zit eigenlijk meer de crux van het verhaal.

Minister **Adriaansens**:
Volgens mij gaat dat dan ook via een platform dat gehouden is aan de regels. Ik wil dat nog wel even checken voor de tweede termijn, maar volgens mij ben je dan net zo goed beschermd. Ja, dat wordt door mijn ambtenaar bevestigd. Dus als het via de platformen gaat, is het aan de importeur.

Voorzitter. De PVV vroeg hoe ik anticipeer op de komende cybersecurityeisen. Volgens mij heb ik daar het nodige over gezegd.

Met het oog op de NIS2 is een herinrichting van CSIRT aangekondigd. Wat is de status, vroeg de heer Valize. Naar verwachting zal ik die NIS2-richtlijn binnenkort met u delen.

(vervolg - loopt door, beurtnummer 14) Minister **Adriaansens**:
Dat wordt in nauwe samenwerking met de departementen uitgevoerd. De uitwerking van dat rapport is erop gericht om organisaties te ondersteunen in het beter beveiligen van systemen, ze te informeren over de kwetsbaarheden en ze bijstand te verlenen als er sprake is van een incident.

Voorzitter. Mevrouw Kathmann vroeg naar de bereidheid om binnen Europa aan te dringen op hogere standaarden. Volgens mij heb ik daar het nodige over gezegd. Ik zie dat hierin wat herhaling zit van wat ik al eerder heb vermeld. Daarmee ben ik door het tweede mapje heen.

Voorzitter. Dan kom ik bij pijler III van de Cybersecuritystrategie. De heer Six Dijkstra vroeg naar het standpunt van de Taskforce Economische Veiligheid. Het staande kabinetsbeleid bij het inkopen en gebruiken van producten en diensten is dat er per casus wordt bezien of er in relatie tot producten en diensten risico's zijn voor de nationale veiligheid en hoe deze beheersbaar kunnen worden gemaakt. Het is niet bij voorbaat zo -- we hebben daar eigenlijk net al het nodige over gezegd -- dat producten uit een bepaald land veiligheidsrisico's met zich meebrengen. Dat is eigenlijk ook wel het standpunt van de Taskforce Economische Veiligheid. Als ik dit zo doorneem,

denk ik dat we gedeeld hebben dat we een open economie zijn en dat we dus die balans en proportionaliteit proberen te zoeken.

De heer **Six Dijkstra** (NSC):
Dan zou ik de minister toch willen vragen of zij een voorbeeld kan noemen van een situatie waarbij het bij vitale infrastructuur wel verantwoord zou zijn om een Chinese router te gebruiken.

Minister **Adriaansens**:
Ik zou bijna zeggen: nee, dat kan ik niet op deze manier. Ik moet dat namelijk onderzoeken.

De heer **Six Dijkstra** (NSC):
Zou u dat willen onderzoeken?

Minister **Adriaansens**:
Misschien heb ik even een herfrasering nodig. Zou de heer Six Dijkstra nog even willen benadrukken wat hij precies bedoelt met deze vraag?

De heer **Six Dijkstra** (NSC):
Ik zal 'm herfraseren. Het zit 'm voornamelijk in de hardware die maakt dat een netwerk verbonden is met het internet, de rand van het netwerk. Het lijkt me in principe onverantwoord als een router of een switch van Chinese makelij zorgt dat een bedrijf of overheidsinstantie verbonden is met het internet. Ik zou geen enkele situatie kunnen bedenken waarin je zou zeggen dat het om een vitale instelling gaat als daar wel een Chinese router is. Moeten we op dat gedeelte niet afstappen van het landenneutrale? Dat is mijn vraag aan de minister. Eén tegenvoorbeeld zou genoeg zijn. Ik zou daar wel heel benieuwd naar zijn.

Minister **Adriaansens**:
Ik heb net toegelicht dat we heel erg kijken naar de risico's. Het gaat heel erg over de toepassing. We maken die beoordeling per casus. Als we dat in algemene zin zouden doen, zouden we de andere kant op ook fouten kunnen maken. Dus ik begrijp de vraag van de heer Six Dijkstra. Dit ruikt ernaar dat we onderzoek moeten doen. Volgens mij moeten we dat dan ook doen. We moeten zorgen dat we proportioneel kijken naar wat het risico is, waar het voor gebruikt wordt en in welke toepassing het zit. Zit het in een bepaalde sector? Heeft het te maken met kritieke systemen? Gaat het over vitale infrastructuur? Volgens mij maken al dat soort zaken heel erg uit om dit

proportioneel te bekijken. Ik zie een kleine instemming bij meneer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Sorry voor alle interrupties, voorzitter.

Ja, mijn vraag gaat specifiek over vitale instellingen. En waar wordt het voor gebruikt? Dit gaat om routers. Dit is standaard iets wat gebruikt wordt om met het internet te verbinden. Waarvoor het netwerk dan gebruikt wordt, maakt dan ook minder uit. Dat is alsof je zou zeggen: "Ik wil niet dat inbrekers in mijn woonkamer komen, dus ik doe mijn voordeur goed op slot. De keukendeur maakt niet uit, want het maakt niet uit als ze in mijn keuken komen." Dan ben ik benieuwd of er omstandigheden zijn waaronder je bij vitale infrastructuur voor netwerkdoeleinden wel Chinese apparatuur zou kunnen gebruiken. Als de minister dat niet ter plekke kan aangeven, dan ben ik benieuwd of er dergelijke casuïstiek is.

Minister **Adriaansens**:
Om even in de metafoor te blijven: als je hele dikke betonmuren hebt, kom je er ook niet binnen. Het hangt er dus ook heel erg van af of je in een gesloten of in een open systeem zit. Dat moet je echt per geval bekijken. Voor vitale infrastructuur zijn er sowieso extra eisen die we met elkaar stellen, en voor kritieke processen idem dito. Als het minder kwetsbaar is, dan is er wel wat ruimte. Helaas zijn er ook gevallen bekend waarin we geen echte alternatieven hebben. Dan moet je dus weer een ander soort afweging maken rond de vraag of je beveiligingseisen kunt toevoegen aan het gebruik van een bepaald product. Het luistert dus nogal nauw.

De **voorzitter**:
Uw laatste interruptie op dit punt, meneer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dit zal mijn laatste interruptie zijn. Ik ben dan wel benieuwd hoe de minister dat voor zich ziet. Welke betonlaag zou er dan omheen kunnen zitten waardoor je zou kunnen zeggen: een router voor een vitale instelling kan prima een Chinese router zijn?

Minister **Adriaansens**:
Bijvoorbeeld de RED, de Radio Equipment Directive, geeft in ieder geval al beveiligingseisen aan de voorkant. We moeten dus ook even kijken in welk

tijdpad we ons begeven. Binnen een bepaalde tijd hebben we die eisen die voor alle producten gelden. Daar zal ook deze apparatuur zich aan moeten houden. Als er dan nog extra risico's zijn doordat je in kritieke processen dan wel vitale infrastructuur zit, moeten we misschien nog een extra check doen. Dat gebeurt overigens ook bij de inkoopeisen al. Voor deze sectoren zijn er op basis van alle regelgeving die we hebben ook bij de inkoper en het bedrijf dat het gebruikt al extra zaken die moeten worden gecheckt. Uit welk land komt het? Welke risico's zijn er? Die zaken moeten worden afgebakend dan wel uitgesloten. Ik wil de vraag best nog gerichter beantwoorden, maar dan moet ik even een casus hebben, denk ik, die we dan doorlichten. Het zou heel interessant kunnen zijn om even van binnen en van buiten te bekijken hoe dat er op dit moment uitziet en hoe dat eruitziet over anderhalf jaar. Die uitdaging wil ik wel aangaan. Als de casus de zonet door de heer Six Dijkstra geschetste is, gaan we dat doen. Ik probeer er non-verbaal achter te komen of dit nu een toezegging is van mij of dat dit gewoon een aanbod was dat niet is aangenomen. Dat maakt nogal uit.

Misschien kan ik het nog even toelichten. Wij hebben gekozen voor een risicomanagementsysteem. We hebben niet gekozen voor een zwart-witsysteem waarin op voorhand allerlei apparatuur wordt uitgesloten. Dat risicomanagementsysteem kent een bepaald soort discipline, een bepaald soort gedrag. Dat is per definitie complexer dan een aantal zaken uitsluiten of toelaten. Ik begrijp best dat we dat eigen moeten maken, en dat je aan de voorkant zou kunnen zeggen: hoe kan het nou toch dat je bepaalde scanners hebt van een bepaalde afkomst? Ik krab ook weleens achter mijn oren omdat ik me afvraag: moeten we dat op die manier doen? Maar als je je gaat verdiepen in die casuïstiek, zie je dat er een heleboel factoren meespelen. Dan is het echt de vraag of je, als je iets heel generiek zou afkeuren, bijvoorbeeld in het voorbeeld dat de heer Six Dijkstra geeft, niet onevenredig, disproportioneel bepaalde handelsrelaties of productenstromen verhindert. De schade daarvan kan misschien vele malen groter zijn dan wat je oplost. Daarom kiezen we met elkaar voor een risicogebaseerd systeem. Dat is wel wat ingewikkelder om uit te leggen; dat begrijp ik. Daar zijn we nu ook een beetje mee bezig. Maar het is wel belangrijk dat we kunnen uitleggen hoe we kijken naar dit soort keuzes en gebruik; daarom is de vraag van de heer Six Dijkstra ook terecht. In die zin wil ik de handschoen wel een keer oppakken, als ik dan maar even vooruitstrevend mag zijn.

De **voorzitter**:
Dan kunnen we toch een toezegging noteren aan de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Ik neem die toezegging graag aan. Ik begrijp ook de diplomatieke reden daarachter, hoor. Zou de minister een casus kunnen geven waarin het wél verantwoord is dat er binnen een vitale instelling netwerkapparatuur afkomstig uit China gebruikt zou kunnen worden? Daar ben ik wel benieuwd naar. Onder welke omstandigheden zou dat zijn? Dan krijgen wij als commissie ook meer inzicht in hoe het aanbestedingsbeleid werkt en hoe bijvoorbeeld zo'n toets op nationale veiligheid in de praktijk vorm krijgt. Is zo'n situatie denkbaar?

Minister **Adriaansens**:
Voor alle helderheid: ik zal het volgende doen. Ik zal in de voortgangsrapportage een alinea, een paragraaf opnemen waarin we even een casus langslopen zoals net geschetst. Dan zou ik het niet willen phrasen in de zin van "wat kunnen we doen om dit mogelijk te maken?" maar het willen beschrijven vanuit de vraag: welke acties nemen we om te kijken welke risico's er verbonden zijn aan het aanschaffen van deze routerapparatuur in deze context? Dat zal ik doen; dat is één.

(vervolg - nieuwe alinea, beurtnummer 16) Minister **Adriaansens**:
Twee. Ik denk dat dit een heel interessante vraag kan zijn om mee te nemen in het werkbezoek dat ik heb aangeboden, want het gaat er juist om hoe het er in de praktijk uitziet en hoe we het toepassen. De reflectie vanuit de Kamer kan zeker ook nuttig zijn bij het optimaliseren van die processen.

Voorzitter. Ik ga door met de vraag van D66, die te maken had met de inval in Oekraïne door Rusland. Wat kunnen we doen om op het dreigingsniveau te anticiperen en het naar beneden te krijgen? Dit zit, zoals ik net zei, in pijler III van de Nederlandse Cybersecuritystrategie. Daarin beschrijft het kabinet de aanpak van cyberdreiging door meer zicht en meer grip op de kwaadwillenden, zoals statelijke actoren, maar ook cybercriminelen. Zoals we in de voortgangsrapportage aangeven, lopen er in dat kader diverse trajecten. Zo investeren we in de operationele slagkracht van de AIVD en de MIVD. We onderzoeken een wetsvoorstel over landen met een offensief cyberprogramma: kunnen we daarin actiever zijn? Onderzoeks- en opsporingsactiviteiten van de politie en het Openbaar Ministerie zijn een doorlopende actie. Ook versterken we ons diplomatieke netwerk. Je moet altijd voorzichtig zijn met dit soort uitspraken, maar tot op heden zien we dat de aanval van Rusland op Oekraïne in beperkte mate heeft geleid tot

bepaalde spillovereffecten naar Nederland. Onze alertheid is wel beduidend toegenomen.

Voorzitter. Ik kom bij de vierde pijler, die vooral gaat over cybersecurityspecialisten. Mevrouw Kathmann vroeg: hoe gaan we om met het tekort aan cybersecurityspecialisten? Het is een algemeen probleem dat we te weinig geschoolde cybersecurityprofessionals hebben. Deze professionals zijn wel een essentiële voorwaarde voor cybersecurity. Als een actie uit de strategie heb ik een onderzoek laten uitvoeren naar de kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt, als je het die naam kan geven. Dat rapport ontvangt u binnenkort. We zien dat die vraag steeds toeneemt. Dat heeft natuurlijk ook te maken met de toename van de digitalisering en het feit dat het aanbod niet hard genoeg meegroeit. We zijn geneigd om het probleem van het tekort aan cybersecurityprofessionals als één probleem te zien, maar het is natuurlijk een samenspel van een heleboel uitdagingen. Het gaat eigenlijk over de hele keten van onderwijs tot aan arbeidsmarkt, en vraag en aanbod daar. We hebben al anderhalf jaar een actieplan in uitvoering tegen arbeidsmarkttekorten in algemene zin op het gebied van digitale en technische beroepen. Dat actieplan ziet echt op het hele traject, van scholing tot en met het aan de slag gaan, aan de slag blijven en omscholen. Het is dus niet one size fits all, maar het heeft onze aandacht. Ik rapporteer ook regelmatig over de voortgang van dit actieprogramma.

Ik kom bij het mapje overig. De heer Six Dijkstra vroeg naar inkoop en aanbesteding. Ik heb daar net het nodige over gezegd bij de beantwoording van de andere vragen. Bij de inkoopeisen zit een check op het risico van het land en het kritieke proces. Er zijn ook een quickscan en een handreiking opgeleverd voor de lokale en rijksoverheid om die checks goed te kunnen doen, maar ook voor bedrijven die aanbestedingsplichtig zijn. Daar vallen onder andere de vitale sectoren onder. Ik heb het dan over de op risico gebaseerde checks die we bij inkoop doen.

Een vraag over de Zeekabel Coalitie, naar aanleiding van de aanstelling van de coördinator. Het is in beginsel een private activiteit, maar we gaan ons er wel steeds meer tegenaan bemoeien, omdat we zien hoe belangrijk het is dat onze infrastructuur goed en veilig is. Het ministerie van Economische Zaken probeert partijen die interesse hebben in het realiseren van een aanlanding in Nederland ook zo goed mogelijk te faciliteren. Daarvoor hebben we de

Zeekabel Coalitie, een publiek-private samenwerking die inzet op het stimuleren van zeekabelaanlandingen in Nederland.

(vervolg - loopt door, beurtnummer 17) Minister **Adriaansens**:
Het ministerie van Economische Zaken is een van de leden van die coalitie. We hebben ook budget beschikbaar gesteld voor het aanstellen van een coalitiecoördinator via het Nederlandse Platform voor de InformatieSamenleving, het ECP. Die coördinator is gestart in september. Ik zal u bij de voortgangsrapportage van de Strategie Digitale Economie informeren over de resultaten tot dusver.

Mevrouw Kathmann vroeg naar een reflectie op het softwarelek bij Carrier Global.

De **voorzitter**:
Voordat u hieraan begint, heeft mevrouw Rajkowski een interruptie.

Mevrouw **Rajkowski** (VVD):
Ik weet nog wel dat iedereen -- dat was natuurlijk niet aan de kant van de minister -- twee jaar geleden, als er werd gepraat over zeekabels, dacht van: goh, waarom is dat eigenlijk interessant en moeten we het erover hebben? Gelukkig groeit het besef dat onze digitale economie en fintech-economie daar voor goede en snelle verbindingen van afhankelijk zijn. Kan die coördinator, op het moment dat u die voortgangsrapportage naar de Kamer stuurt … U schreef ook dat de schepen die nodig zijn om dit soort kabels aan te leggen, te onderhouden et cetera de komende tijd zijn volgeboekt. Dat maakt de bewegingsruimte voor Nederlandse investeringen soms dus lastig. Is daar al een update over? Als er toch nog meer kabels vervangen of aangelegd moeten worden of als de aanlanding vanuit Canada geregeld moet worden, is het natuurlijk wel belangrijk dat het inboeken van die kabels snel gebeurt. Kan een update daarover ook in de voortgangsrapportage worden meegenomen?

Minister **Adriaansens**:
Ja, ik neem die update mee.

Mevrouw Kathmann vroeg naar de reflectie. Voor een deel is dat misschien een herhaling van wat we al eerder hebben gedeeld. We zullen kijken of ik daar voldoende aan tegemoet ben gekomen.

De eigenaar of de leverancier van de systemen is primair verantwoordelijk voor de beveiliging van het systeem. In dit geval was er een kwetsbaarheid in de software, die door de ontdekkende partij is gemeld aan Carrier Global en aan SMC Alarmcentrale, die in Nederland veel klanten bedient. Vervolgens is er door beide bedrijven geen actie ondernomen, en dat is kwalijk; laat ik dat hier voor eigen risico en rekening wel uitspreken. Ik vind dat dit zou moeten. We moeten allemaal alert zijn en onze verantwoordelijkheid nemen. Het helpt enorm als iedereen dat doet. Het in de media bekendmaken van een kwetsbaarheid is voor de ontdekker eigenlijk de laatste stok achter de deur om bedrijven te motiveren om die aan te pakken. De melder heeft die stap ondernomen en dat is dan ook terecht. Op die manier werkt ons systeem. Maar ook het Nationaal Cyber Security Centrum kan een rol vervullen, als intermediair, indien de melder van een kwetsbaarheid en het bedrijf er samen niet uitkomen.

In dit geval is pas na het melden aan de media contact gezocht met het Nationaal Cyber Security Centrum. Er is toen een zogenaamde Coordinated Vulnerability Disclosure-melding ingediend. Het Nationaal Cyber Security Centrum kan dan contact opnemen met SMC Nederland om afspraken te maken over hoe ermee om te gaan. Het is nu primair aan Carrier Global en SMC om intern te onderzoeken waarom de melding van die kwetsbaarheid niet heeft geleid tot actie en om ervoor te zorgen dat er in de toekomst beter op wordt geacteerd. Dat is de reflectie. Ik hoop ook dat dit, doordat er ruchtbaarheid aan is gegeven, leidt tot alertheid bij andere bedrijven. We hoeven namelijk niet altijd te denken dat het van kwade zin is; soms is er ook onvoldoende bewustzijn van de verantwoordelijkheid om deze informatie te delen.

Dan ga ik naar de vraag van de heer Valize wanneer het onderzoek rondom artificial intelligence, AI, en cybersecurity klaar is. Het ministerie van EZK heeft TNO de opdracht gegeven om een verkenning uit te voeren naar de impact van AI op cybersecurity. In die verkenning werken we samen met overheidspartners, kennispartners en het bedrijfsleven. Er wordt een rapport over opgemaakt. Ik verwacht dat die verkenning vóór de zomer kan worden gedeeld met uw Kamer.

Voorzitter. De heer Six Dijkstra vroeg hoe we ervoor zorgen dat principes zoals security first niet alleen beleid zijn, maar ook daadwerkelijk worden uitgevoerd. Ik ben het er volledig mee eens dat we moeten zorgen dat het geen papieren tijger wordt en dat er daadwerkelijk actie wordt uitgevoerd.

We moeten handelen op dreigingen en de preventie daarvan. Maar ik denk ook dat we met de verschillende bestaande en zeker ook de komende Europese wet- en regelgeving op het gebied van digitale weerbaarheid laten zien dat die vrijblijvendheid echt wel voorbij is. Dat gaat bijvoorbeeld om NIS2 en CRA. De onafhankelijk toezichthouders, in dit geval de RDI, zijn essentieel om deze regels te laten slagen en effectief laten zijn.

(vervolg - nieuwe alinea, beurtnummer 18) Minister **Adriaansens**:
Voorzitter. Mevrouw Kathmann vroeg nog hoe vrije opensourcesoftware een bijdrage kan leveren aan de cybersecurity van de overheid en hoe we die zo proactief mogelijk kunnen aanbieden. In oktober 2022 heeft het ministerie van Binnenlandse Zaken een opensourcestrategie gepubliceerd. Onderdeel daarvan is een afwegingskader met een stappenplan om ervoor te zorgen dat overheidsprofessionals zo goed mogelijk uitvoering geven aan het "open source tenzij"-beleid. Dat beleid kent het uitgangspunt dat overheden worden opgeroepen om de broncode van open software die ontwikkeld is met publieke middelen zo veel mogelijk open source te publiceren, en dus ook bij software ten behoeve van de cybersecurity van de overheid. Er bestaan ook wel al verschillende voorbeelden van opensourcesoftware vanuit de overheid voor cybersecurity, zoals het project OpenKAT -- KAT is de afkorting voor kwetsbaarhedenanalysetool -- of internet.nl.

Daarmee, voorzitter, ben ik door de aan mij gestelde vragen heen, voor zover ik het kan overzien.

De **voorzitter**:
Ik kijk even naar links. Ik zie inderdaad dat iedereen tevreden is over de beantwoording van de vragen. Dat brengt ons dus eigenlijk meteen bij de tweede termijn. Voor mevrouw Rajkowski hoeft het niet. Dan is het woord aan de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank u wel, voorzitter. Wederom dank aan de minister voor de beantwoording. We hebben het over veel onderwerpen gehad. Ik wil toch nog even stilstaan bij -- u raadt het al --- het landenneutrale beleid. Ik zie uit naar de casus die onze kant op komt bij het volgende document dat richting de Kamer gaat. Ik heb dan toch nog wel een vraag bij het inkoop- en aanbestedingsproces voor kritieke en vitale infrastructuur. Nu staat het zo beschreven dat nationale veiligheid een overweging is om mee te nemen, maar als we naar "security first" toegaan, zou die wel het uitgangspunt

moeten zijn. Hoe komen we uiteindelijk, met de Europese wet- en regelgeving, maar ook met de ABRO, op een punt waarop dat de norm is bij het aanbestedingsproces? Daar zou ik toch wel benieuwd naar zijn. Misschien kan dat ook nog meegenomen worden in die casus.

Een tweede vraag die ik nog had, ziet op de NIS2 en andere wet- en regelgeving. De implementatie daarvan laat nog weleens op zich wachten. Dat lijkt wel een patroon te zijn. Dat komt natuurlijk ten dele door de sectorale toezichthouders. Maar mijn vraag ging ook over het volgende. De verantwoordelijken voor het beleid en de uitvoering in Nederland ten aanzien van cybersecurity, en alle rollen daarbij, zijn bij Nederlandse partijen best verspreid over veel overheidsonderdelen. Deelt de minister dat, en denkt zij dat dat van invloed is op de lange duur van de termijnen voor implementatie?

Voorzitter. Ik zou bij dezen ook graag een tweeminutendebat willen aanvragen om dit eventueel nog voort te zetten.

Dank u wel.

De **voorzitter**:
Dan is het woord aan mevrouw Van der Werf van D66.

Mevrouw **Van der Werf** (D66):
Dank u wel, voorzitter. Dank aan de minister voor de overzichtelijke beantwoording. Ik kan me voorstellen dat dit voor haar soms ook wat onoverzichtelijk is, aangezien het voor een groot deel natuurlijk helemaal niet op haar beleidsterrein lag. Dank daarvoor dus.

Ik wilde op drie punten nog even terugkomen. We hadden het over de Nederlandse Cybersecuritystrategie en de extra middelen. Zij hebben natuurlijk die oproep aan het kabinet gedaan. U gaf aan: we zijn daarmee bezig en hebben daar geld voor gereserveerd. Maar wat zij vragen, is natuurlijk niet niks. Zij zeggen: in 2024 is er eigenlijk al 200 miljoen extra nodig, oplopend tot 550 miljoen in 2028. Dat is natuurlijk een oproep waaraan op dit moment nog geen gehoor wordt gegeven. Nu hoeven we natuurlijk niet een-op-een alles over te nemen wat er uit het veld komt, maar ik was wel benieuwd of u nog even kunt duiden in hoeverre dat nodig is, en waarop u dan anticipeert.

Het tweede punt betreft NIS2, waarover we het al hadden. Ik ben niet helemaal gerustgesteld over de timing, ook al gaf u aan dat u best iets in een tijdpad zou kunnen aangeven. Het is natuurlijk ook lastig, want de minister van JenV is hierbij niet aanwezig, maar ik overweeg wel een motie om dit toch tijdig voor elkaar te hebben in Nederland. Daarom sluit ik me graag aan bij het verzoek om het tweeminutendebat dat mijn buurman al deed.

(vervolg - nieuwe alinea, beurtnummer 19) Mevrouw **Van der Werf** (D66):
Het derde punt is de aangifte en pakkans bij slachtoffers van datalekken en bedrijven. U gaf aan: wij moedigen mensen natuurlijk van harte aan om aangifte te doen. Dat begrijp ik. Het belang daarvan wil ik vanaf deze plaats ook nogmaals benadrukken. Maar op het moment dat mensen weten dat de pakkans ongeveer 10% is, werkt dat natuurlijk niet heel motiverend voor het doen van die aangifte. Er zal dus ook iets moeten gebeuren aan die kant, aan het vergroten van de pakkans en misschien ook aan het vergroten van de expertise bij het opnemen van die aangiften, maar het antwoord daarover vond ik nog wat mager. Wat betreft alleen online meldingen kunnen doen weten we namelijk ook van mensen hoelang het soms kan duren voor je daar weer wat van hoort. Ik zou daarop dus graag wat meer inzet van het kabinet zien.

De **voorzitter**:
Dan is het woord aan de heer Valize van de PVV.

De heer **Valize** (PVV):
Dank, voorzitter. Dank voor het woord. Dank ook aan de minister voor de heldere beantwoording van de vele vragen die gesteld zijn. Ik heb toch nog een kleine vraag met betrekking tot de platformen, een eerder genoemd onderwerp. Er zijn diverse platformen. Die zijn niet allemaal gestationeerd in Europa. Ik ben dus benieuwd hoe dat dadelijk met die Cyber Resilience Act gaat werken voor platformen die buiten de Europese Unie vallen. Dat was mijn laatste vraag.

De **voorzitter**:
Dank u wel. Ik wil mevrouw Rajkowski vragen of zij even de voorzittershamer wil overnemen om mij het woord te geven.

Voorzitter: Rajkowski

De **voorzitter**:
Ja, hoor. Dank. Dan geef ik nu het woord aan mevrouw Kathmann van GroenLinks-PvdA voor haar tweede termijn.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik gebruik mijn tweede termijn ook om vragen te stellen bij de vragen die ik net heb gesteld, want sommige waren misschien niet duidelijk genoeg; dat is altijd een beetje lastig als je voorzitter bent. De vraag over de opensourcesoftware lag namelijk vooral in het verlengde van de constatering dat het er op heel veel vlakken gewoon toe doet hoe dik je portemonnee is. Of je geld hebt of niet, doet er ook gewoon toe voor je cyberveiligheid. Opensourcesoftware kan ongelofelijk helpen bij de cyberveiligheid van mensen die misschien niet het geld hebben om al die pakketjes aan te schaffen. Datzelfde geldt voor al die punten die we hebben om mensen te helpen met digitalisering. Kan er van daaruit niet actiever gestuurd worden op de cyberveiligheid, op de gratis alternatieven om die mensen te helpen? Daarover ging die vraag dus.

Dan wat betreft die ethische hackers. Dat weet ik; er wordt samengewerkt met ethische hackers bij het NCSC. Maar mijn vraag was veel meer gesteld vanuit de kant van mkb'ers. Ethische hackers inhuren is gewoon ongelofelijk duur. Het zou mkb'ers kunnen helpen als die niet alleen maar bij NCSC zitten om die dreigingsinfo in beeld te krijgen en te delen, maar als mkb'ers daar ook gebruik van kunnen maken bij sommige dingen. Misschien zeggen mkb'ers collectief, in een sector of bijvoorbeeld bij een alarmsysteem gewoon eens: we willen dat laten hacken omdat we willen weten waar de kwetsbaarheden zitten. Het zou goed zijn als dat ook proactief kan worden uitgevraagd, als een soort steun voor die mkb'er, die vaak in zijn eentje of zelfs met zijn tienen niet het geld heeft om dat goed te doen. Daar was mijn vraag dus eigenlijk op gericht.

Dan die vraag over dat label. Eigenlijk ben ik het wel eens met het antwoord van de minister dat de verantwoordelijkheid inderdaad bij de fabrikant ligt. Dat is mooi. We gaan iets meer snelheid maken voor die draadloze apparaten. Dat komt in 2025. Zou dat dan ook al voor meerdere apparaten kunnen gaan gelden of wordt dat echt te kort dag?

Dan het antwoord over het melden bij de AP. Dat is in ieder geval goed, maar dat gaat over gevallen waarbij persoonsgegevens in het gedrang zijn. Maar wat nou als het gaat om lekken in software die geen gevolgen hebben voor

persoonsgegevens, maar waarbij het gaat om een lek in servicesoftware waardoor ransomware kan worden geïnstalleerd? Waar ga je dan heen? Weet iedereen ook goed genoeg waar je die melding kan doen?

Dan mijn vraag over die tekorten op de arbeidsmarkt. Fijn dat dat rapport er is en dat die bevindingen er snel aankomen. Ik ben in ieder geval benieuwd. Ik hoop dat het gewoon beter gaat sinds er een actieplan is, maar ik heb vooral de vraag: krijgen we nou de stand van zaken wat betreft die cyberella's? Zitten die in het rapport? We hebben het namelijk steeds vaker over apps, bijvoorbeeld voor digitale zorg. Als daar gewoon te weinig vrouwen aan werken, dan krijg je soms misschien zelfs wel apps die voor vrouwen helemaal niet van toepassing zijn. Meer vrouwen zou dus gewoon ongelofelijk fijn zijn, niet alleen in de cybersecuritysector, maar in de hele ICT-sector.

De **voorzitter**:
Dan geef ik bij dezen de voorzittershamer weer terug.

Voorzitter: Kathmann

De **voorzitter**:
Dank u wel. Er is een interruptie van de heer Valize van de PVV.

De heer **Valize** (PVV):
Aangezien ik mijn spreektijd net al heb gebruikt, wil ik graag een vraag stellen aan mevrouw Kathmann met doorverwijzing naar de minister, als het mij wordt toegestaan. U hebt het ook even gehad over het logo, maar wij zien dat het CE-logo heel verwarrend is, want je hebt dus China Export en je hebt de Conformité Européenne. Bent u het ermee eens dat daar ook weleens wat aandacht voor mag komen?

De **voorzitter**:
Meneer Valize, ik dank u voor deze vraag. Ik ben het daarmee eens en ik zou eigenlijk aan de minister willen vragen of die het daar ook mee eens is. Dat brengt ons bij de beantwoording. De minister heeft vijf minuten nodig. Dat is goed. Dan schorsen we de vergadering voor vijf minuten.

De vergadering wordt van 15.02 uur tot 15.15 uur geschorst.

De **voorzitter**:
De minister is klaar voor de beantwoording.

Minister **Adriaansens**:
Dank u wel. Het gaat snel, voorzitter. Als ik niet precies alle vragen heb, zult u mij vast corrigeren.

Allereerst de heer Six Dijkstra. Kunnen we nou niet zorgen dat we security first centraal zetten bij inkoop en aanbesteding? We zien inderdaad dat het risico steeds groter wordt, dus ik denk dat het logisch is dat die vraag voorkomt. De ABRO is daar juist voor bedoeld. Die is bedoeld om te zorgen dat we heel gericht kijken naar de cybersecurityrisico's. Maar het voorstel om nationale veiligheid als bindende voorwaarde te zien bij inkoop en aanbesteding, vind ik interessant. Ik wil dat dus wel explicieter meenemen om te kijken of dat voldoende plek heeft of dat we daar nog iets aan moeten doen.

Voorzitter. Dan de NIS2. Helaas gaat dat niet sneller. Ik heb geprobeerd dat uit te leggen. In Nederland doen we dat heel specifiek, per sector. We willen de bestaande toezichthouders ook faciliteren en zorgen dat zij goed toezicht kunnen houden, en we willen de NIS dus goed gaan implementeren. Maar ondertussen doen we al het nodige. We zijn bezig met het implementeren van een risicomanagementsysteem en er zijn trainingen. Dat alles doen we met de bedoeling dat we een vliegende start hebben en daadwerkelijk klaar zijn als die wet dadelijk geïmplementeerd is. Dus ik begrijp het signaal, maar met de zorgvuldigheid die wij nu betrachten, is dit echt het hoogst haalbare. Ik heb de termijnen van die wet in de eerste termijn geschetst.

Dan was er een vraag over het geld. Stellen we het DTC voldoende in staat om het werk te doen? Dit kabinet heeft structureel 111 miljoen uitgetrokken voor het versterken van de cybersecurity. Het is uiteraard aan een volgend kabinet om dat eventueel te verzwaren. Ik heb op dit moment geen signalen dat het met het huidige takenpakket niet zou lukken.

D66 vroeg naar de pakkans. Ja, ik begrijp die zorg. Ik denk dat we die allemaal onderschrijven. Zoals u terecht aangaf, heeft het een aantal kanten. Het gaat over melding doen. Dat kunnen we makkelijker maken door het mogelijk te maken om online melding te doen van een risico of crimineel gedrag. Aan de andere kant willen we natuurlijk ook dat het opgepakt wordt. Op dit moment is de pakkans wel laag. Dat onderschrijf ik dus. Ik weet dat bij

het Openbaar Ministerie en de politie hard wordt gewerkt aan het versterken van deze capaciteit. Maar ja, we moeten ook realistisch zijn; de tekorten die er zijn op de arbeidsmarkt überhaupt en specifiek wat betreft deze kennis, gelden hiervoor ook. Desalniettemin zijn we aan het kijken hoe we de keten kunnen versterken. Zo weet ik dat het DTC betrokken is bij een project, samen met onder andere de politie en het mkb, om betere ondersteuning te geven aan het mkb. Dat zijn twee pilots, in Noord-Nederland en in Oost-Nederland. Dat gaat ook over hoe je dit aan de preventieve kant goed kan doen en hoe de politie kennis kan nemen van de risico's en dreigingen die worden ervaren, zodat we toch die expertise bouwen met praktijkkennis.

Dan ten aanzien van de platforms, zoals Ali. Als een platform in Europa een product hier verkoopt, dan moet het aan de eisen voldoen. Als je zelf een pakje koopt in China, dan koop je een pakje in China, zou ik bijna zeggen. Dat is wat het is. Ik hou er wel van om het niet te verbloemen. Volgens mij is dat dan wat het is. In de Europese Unie versterken en verstevigen wij de veiligheid. Daar is onze regelgeving ook op gericht.

Dan open source. We kunnen dat niet verplichten, maar we kunnen dat natuurlijk wel bevorderen. Voor dat laatste ben ik zeer gemotiveerd, bijvoorbeeld in aanbestedingen. Dan zorg je dat je, als ermee wordt gewerkt, open source bevordert als dat kan, en ook dat dat beschikbaar wordt gesteld.

Dan de vraag rondom ethisch hacken. Het inhuren daarvan is enorm duur. Dat klopt, maar je kan wel een vraag stellen aan het DTC. Dat kan je individueel en collectief doen. We hebben een project, Cyclotron, waarin we met verschillende bedrijven, overheidsinstellingen en kennisinstellingen met zo'n algemeen softwareprobleem aan de slag gaan, dat analyseren en kijken wat daaraan te doen valt. Er is dus wel degelijk een manier om niet zelf die kosten te maken, maar het collectief te vragen.

(vervolg - nieuwe alinea, beurtnummer 22) Minister **Adriaansens**:
Voorzitter. De vraag rondom de labels. Ik heb in de randen van dit debat eventjes gedeeld dat het met het tijdpad dat voorligt niet haalbaar is om de aparte certificeringssystemen nu te versnellen en naar voren te halen.

Dan de lekken in de software, die gevolgen hebben voor ransomware. Is bekend waar je je moet melden als je ethisch hacker bent? Dat is bij het DIVD en het NCSC. Mij is bekend dat hackers dit wel weten en als je het niet weet,

dan is er op de websites van deze organisaties voldoende te vinden zodat je weet waar je heen moet. Maar de ervaring leert dat dit werkt.

Dan komen we bij de cyberella's en het tekort op de arbeidsmarkt. Ik vind het woord erg leuk, dus we gaan eens kijken of we daar wat mee kunnen. Ik denk inderdaad dat het volstrekt terecht is dat we dat bevorderen. We zullen eens even kijken of we er wat creativiteit in kunnen brengen om meer vrouwen in de cyber aan de slag te krijgen. Ik denk dat dat heel belangrijk is. Het zat ook in het rapport, dus het wordt binnenkort ook gestuurd aan uw Kamer en dan kunnen we kijken of daar nog goede ideeën aan toe te voegen zijn.

Dan ten aanzien van het CE- en het China Export-logo en de verwarring daaromtrent. Dat is een volstrekt terecht punt. Wij zaten hier ook net te puzzelen op de vraag: wat doe je daar nou mee? Want als het commercieel is, dan kan je daar natuurlijk een zaak van maken. Dan kun je zeggen: dat bedrijf hanteert een logo dat heel erg lijkt op dat van mijn bedrijf en ik was eerder, dus die ander moet daarmee ophouden. Dat is eigenlijk zoals het werkt. Dan moet de rechter het daarmee eens zijn. Hier gaat het natuurlijk over een overheidsactiviteit. Ik weet niet precies welke weg daar dan het beste voorligt. Ik vind het wel zorgelijk, want met een logo probeer je natuurlijk een bepaald soort veiligheid uit te stralen en als dat nepveiligheid is, dan ben je nog verder van huis. Ik zal dit in de Europese Unie aankaarten. Hebben zij al acties ondernomen om deze verwarring tegen te gaan? Zo nee, kunnen wij er dan nog iets aan doen? Ik denk wel dat er in dit geval Europees iets zou moeten worden gedaan. Maar het is wel duidelijk dat er iets moet gebeuren. Ik zal het aankaarten, navragen en er dan over rapporteren en eventueel zelf iets in gang zetten.

Dat waren de vragen, voorzitter.

De **voorzitter**:
Dan is er nog een vraag van de heer Six Dijkstra van NSC.

De heer **Six Dijkstra** (NSC):
Ik meen dat ik één onbeantwoorde vraag heb. Die had te maken met de verantwoordelijkheidsverdeling voor cyberbeleid en de uitvoering daarvan in Nederland, anders dan de sectorale toezichthouders. Dus het gaat om de functionele rollen. Ik kan dat nog verder toelichten als de minister daar behoefte aan heeft.

Minister **Adriaansens**:
Ik denk dat dat helpt, want anders ga ik weer een algemeen antwoord geven en daar bent u niet bij gebaat.

De heer **Six Dijkstra** (NSC):
Het zit 'm voornamelijk in een aantal rollen die in Nederland allemaal bij aparte instanties zijn belegd, terwijl mijn gevoel zegt -- dat kan nader onderzocht worden -- dat dat in andere landen vaak meer gecentraliseerd is. De beleidsverantwoordelijke voor de Nationale Cybersecurity Agenda is in Nederland bijvoorbeeld de NCTV, maar voor het nationale CSIRT is dat dan weer het NCSC en het CSIRT-DSP. Voor de National Cybersecurity Certification Authority is dan weer de RDI verantwoordelijk. Voor het National Coordination Center is het weer de RVO. Uiteindelijk heb je ook nog de National Security Authority, de NSA, die in Nederland onder de AIVD valt. Dat zijn heel veel instanties: zes instanties voor vijf taken. Ik heb het idee dat dat in andere landen anders belegd is. Is daar al eens naar gekeken?

Minister **Adriaansens**:
Dan begrijp ik uw vraag toch goed. Dat klopt. We hebben in Nederland echt kwalitatief hoogstaande organisaties, waarvan u er een aantal noemt. We hebben ervoor gekozen om de bestaande structuur te versterken, maar dat is een keuze. Dat leidt tot een bepaalde vertraging in de eerste fase, maar hopelijk tot een versnelling in de fase dat we dat geïmplementeerd hebben. Het heeft er ook mee te maken dat een sectorspecifieke verdeling vaak ook betere communicatie met de achterban geeft. Je kan dus als je in de zorg werkt bijvoorbeeld veel meer inspelen op de daadwerkelijke behoeften van zorgorganisaties. Als je in de infrastructuur zit idem dito. Er is dus wel degelijk over nagedacht en er is voor gekozen om niet weer een nieuwe structuur te bouwen, waar je dan overigens ook heel veel tijd mee kwijt bent, maar om deze wet- en regelgeving op basis van de bestaande structuur in te voeren. Ik ben het er wel mee eens dat dat, als je het zo schetst, wel een heel versnipperd beeld geeft. Desalniettemin wordt er natuurlijk ook gecoördineerd door de RDI en dadelijk door de integrale organisatie op het gebied van cybersecurity. Daar waar we kunnen, integreren we de activiteiten dus ook daadwerkelijk. Zolang ik hier zit, zal dat ook mijn insteek zijn, om ervoor te zorgen dat het wel overzichtelijk blijft.

(vervolg - loopt door, beurtnummer 23) Minister **Adriaansens**:
In die zin ben ik ook enthousiast over de integratie van het DTC, het NCSC en zo verder. Daar waar het kan, moet je dat bundelen.

De heer **Six Dijkstra** (NSC):
Dank, helder. Ik begrijp inderdaad dat dat een keuze is die ooit gemaakt is. Ik ben wel benieuwd of de minister kan onderbouwen dat dit in een later stadium inderdaad tot versnelling leidt ten opzichte van nabuurlanden.

Minister **Adriaansens**:
Ik stel voor dat ik in de najaarsrapportage, waarin ik jaarlijks rapporteer over de voortgang van de acties, met name naar aanleiding van de integratie van het DTC, het NCSC et cetera, nog eens reflecteer op deze vraag en aangeef dat in de Kamer is gevraagd hoe je kan bevorderen dat ons systeem uiteindelijk gaat werken en die versnelling oplevert. Ik bedoel dus eigenlijk een bevestiging van de structuur. Ik zou daaraan toe willen voegen "en daar waar mogelijk samenvoegen", maar ik zal ook uitleggen waarom we dat verschil hanteren om bijvoorbeeld de achterbannen, die echt heel anders zijn, te bereiken.

De **voorzitter**:
Dan kijk ik naar links. Volgens mij zijn alle vragen beantwoord. Ik dank de minister voor de beantwoording. Ik hoorde hier links van mij al iemand zeggen dat dat als een toezegging klinkt. We kijken inderdaad even naar de toezeggingen.

Het lid Six Dijkstra heeft een tweeminutendebat aangevraagd.

- De minister zegt toe in de volgende voortgangsrapportage van de NLCS de conclusies en aanbevelingen uit het rapport van Dialogic mee te nemen.
- De minister zegt toe dat in de volgende voortgangsrapportage van de NLCS een casus wordt opgenomen naar aanleiding van de genoemde punten van het lid Six Dijkstra, met betrekking tot de risico's van het gebruik van mogelijk onveilige apparaten verbonden met het internet, zoals routers en security first, bij aanbestedingen.

Ja, ze knikken allebei.

- De minister zegt toe dat in de volgende voortgangsrapportage van de NLCS het bestuurlijk convenant digitale veiligheid wordt meegenomen.
- De minister zegt toe dat in de volgende voortgangsrapportage Strategie Digitale Economie over de voortgang en rapportage van de

nieuw aangestelde coördinator van de Zeekabel Coalitie wordt geïnformeerd. Hierin wordt ook een update opgenomen met betrekking tot het genoemde punt van het lid Rajkowski over het aanleggen/vervangen van nieuwe zeekabels.

- De minister zegt ook toe dat het onderzoek over de samenhang tussen AI en cybersecurity voor de zomer met de Kamer wordt gedeeld.
- De minister zegt toe dat de Kamer binnenkort een onderzoek ontvangt over het tekort aan cybersecurityprofessionals op de arbeidsmarkt. Er staat tussen haakjes: "tijdpad?".
- De minister zegt toe in de najaarsrapportage te reflecteren op de vraag van het lid Six Dijkstra met betrekking tot de decentralisatie aangaande cybersecuritytoezichthouders.

Ja? Ik zie iedereen knikken. Dan hebben we ook de toezeggingen gehad.

Minister **Adriaansens**:
Het tijdpad was voor de zomer, hè?

De **voorzitter**:
Ja. Dank u wel.

Sluiting 15.27 uur.