Tweede Kamer, Online veiligheid en cybersecurity

VERSLAG VAN EEN COMMISSIEDEBAT
Concept

De vaste commissie voor Digitale Zaken heeft op 5 februari 2025 overleg gevoerd met de heer Beljaarts, minister van Economische Zaken, en de heer Van Weel, minister van Justitie en Veiligheid, over:

- **de brief van de minister van Justitie en Veiligheid d.d. 23 mei 2024 inzake toekomstvisie Cyberweerbaarheidsnetwerk (26643, nr. 1176);**
- **de brief van de minister van Economische Zaken en Klimaat d.d. 19 juni 2024 inzake antwoorden op vragen commissie van de V-100 over het thema Cyberweerbaarheid, mkb en data-encryptie (36560-XIII, nr. 8);**
- **de brief van de minister van Justitie en Veiligheid d.d. 17 juni 2024 inzake Samenhangend Inspectiebeeld cybersecurity vitale processen (26643, nr. 1194);**
- **de brief van de minister van Economische Zaken en Klimaat d.d. 7 juni 2024 inzake Nationale Technologiestrategie - agenda Cybersecurity Technologies (26643, nr. 1183);**
- **de brief van de minister van Justitie en Veiligheid d.d. 19 juli 2024 inzake computerstoring CrowdStrike (26643, nr. 1212);**
- **de brief van de minister van Justitie en Veiligheid d.d. 2 september 2024 inzake evaluatie ISIDOOR IV (26643, nr. 1216);**
- **de brief van de minister van Justitie en Veiligheid d.d. 16 oktober 2024 inzake gevolgen niet-tijdige implementatie NIS2- en CER-richtlijn (22112, nr. 3968);**
- **de brief van de minister van Justitie en Veiligheid d.d. 28 oktober 2024 inzake Cybersecuritybeeld Nederland 2024 en voortgang Nederlandse Cybersecuritystrategie (26643, nr. 1229).**

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

De voorzitter van de vaste commissie voor Digitale Zaken,
Wingelaar

De griffier van de vaste commissie voor Digitale Zaken,
Boeve

Voorzitter: Valize
Griffier: Muller

Aanwezig zijn vijf leden der Kamer, te weten: Kathmann, Koekkoek, Michon-Derkzen, Six Dijkstra en Valize,

en de heer Beljaarts, minister van Economische Zaken, en de heer Van Weel, minister van Justitie en Veiligheid.

Aanvang 13.00 uur.

De **voorzitter**:
Goedemiddag allemaal. Welkom op deze woensdagmiddag 5 februari 2025. Het is 13.00 uur geweest. Vandaag staat voor de commissie Digitale Zaken op de agenda een commissiedebat over online veiligheid en cybersecurity. Aan de zijde van het kabinet zijn aangeschoven minister Van Weel van Justitie en Veiligheid en minister Beljaarts van Economische Zaken. Van de zijde van de Kamer zijn inmiddels aangeschoven de heer Six Dijkstra namens Nieuw Sociaal Contract en mevrouw Michon-Derkzen namens de Volkspartij voor Vrijheid en Democratie. Zelf zal ik dadelijk ook nog het woord voeren. Dan zal ik het voorzitterschap heel even overdragen aan de heer Six Dijkstra. Ik stel voor om te beginnen met de aftrap door de heer Six Dijkstra, die zijn inbreng zal doen namens Nieuw Sociaal Contract. Excuseer, nog een klein punt: we stellen voor om vier interrupties per spreker toe te staan.

De heer **Six Dijkstra** (NSC):
Dank u wel, voorzitter. Ik zal aftrappen. Goed dat we vandaag over dit belangrijke thema van cybersecurity spreken. Laat ik beginnen met het zogeheten laaghangend fruit. Uit eerder onderzoek van de Autoriteit Persoonsgegevens — ik heb het eerder aangehaald — blijkt dat bij 70% van de ransomewareaanvallen de cyberbasishygiëne, om het zo te zeggen, niet op orde is. Het gaat echt om basale dingen: een slecht wachtwoordbeleid, geen meerfactorauthenticatie, updates die niet op tijd worden uitgevoerd en, in het geval van een groot bedrijf, niet voldoende netwerksegmentatie. Daar is dus nog heel veel winst te behalen. Er komt natuurlijk heel veel regelgeving vanuit Europa op Nederlandse organisaties af en ik hoor vaak dat instanties door de bomen het bos niet meer zien, maar ik denk dat met een paar kleine ingrepen al heel veel bescherming mogelijk is. Hoe gaan we bevorderen dat organisaties in die hele wirwar van regelgeving die op ze afkomt zich er in ieder geval van bewust zijn dat die paar concrete stappen op orde moeten zijn? Kunnen we bijvoorbeeld ook de winst inzichtelijk maken als dit wél op orde is? Heeft de minister van Justitie bijvoorbeeld een inschatting van wat het de Nederlandse samenleving aan datalekken zou schelen of wat het het bedrijfsleven zou schelen aan losgeld dat ze zouden moeten overmaken voor ransomware?

Is het kabinet het met mij eens dat het de norm zou moeten zijn dat ook op bestuurlijk niveau beveiliging, en zeker digitale beveiliging, de hoogste aandacht geniet? We hebben bij het NCTV-schandaal gezien hoe het mis kan gaan. Als er geen aandacht is voor de basisbeveiliging van een departement, dan lekken al onze staatsgeheimen uit naar de Marokkaanse inlichtingendienst. Maar daar komen we nog over te spreken. Mijn concrete vraag voor nu is: hoe gaat het kabinet uitdragen dat in dit zeer gedigitaliseerde land de norm wordt dat IT en cyberveiligheid bestuurlijk een thema wordt, een thema waar het management actief op stuurt? Hoe kijkt de minister van Justitie bijvoorbeeld aan tegen het Reporting Initiative van de Werkgroep NOREA voor een verslaggevingsstandaard voor IT-onderwerpen, zodat gestandaardiseerd kan worden gestuurd op de IT van een bedrijf?

Voorzitter. Ik wil het graag nog hebben over kwantumveiligheid. We hebben vorige week al gedebatteerd met de staatssecretaris Digitalisering over de migratie van de overheid naar kwantumveilige cryptografie. Het is belangrijk dat de samenleving beschermd wordt tegen de komst van een kwantumcomputer die al onze encryptie kan breken en in potentie grote delen van de samenleving onveilig maakt. Die migratie is dus heel

belangrijk. Tegelijkertijd kan "Q-day", zoals dat wordt genoemd, het moment dat de kwantumcomputer er is, hoe dan ook heel impactvol zijn. We hebben ook de zogeheten "store now, decrypt later"-aanvallen, waarbij statelijke actoren — denk aan China, denk aan Rusland — heel veel data die nu versleuteld zijn, opslaan, jarenlang bewaren en de encryptie doorbreken als die kwantumcomputer er eenmaal is. Om dat te mitigeren gaan heel veel grote bedrijven — denk aan internetbrowsers, denk aan chatapplicaties als WhatsApp en Signal — nu over, of hebben ze dat al gedaan, op kwantumveilige standaarden. Maar dat "store now, decrypt later" is een reëel gevaar, ook als mensen al over zijn. Want als die data geharvest zijn en de encryptie doorbroken wordt, heeft dat over vijf, tien of wie weet hoeveel jaar gewoon impact op de samenleving. Daar zitten namelijk ook data tussen die we dan nog steeds vertrouwelijk zouden willen zien. Het zou chaos in de samenleving kunnen veroorzaken als persoonlijke gesprekken van mensen op straat komen te liggen of als al het internetgedrag van mensen in de openbaarheid komt. Dat is best een reëel scenario, als ik het zo zie. Dus ook als alles goed gaat qua kwantummigratie — dat is een vrij utopisch idee — kan het nog steeds een grote impact hebben. Is het kabinet daarom bereid om impactscenario's uit te werken voor de situatie dat Q-day er is en "store now, decrypt later"-aanvallen door Rusland, China of andere actoren uitgevoerd worden? Hoe zou dat de samenleving kunnen ontwrichten? Hoe zouden we daarop goed voorbereid kunnen zijn?

Voorzitter. Dan een laatste punt. Ik weet dat het iets meer aan cybercrime dan cybersecurity raakt. Maar aangezien de minister van JenV er is, voel ik toch de ruimte om de vraag te stellen. Een contact van mij in de cybersecuritysector geeft aan, op basis van onderzoek op het darkweb, dat naast alle grote spelers, statelijke actoren en grote criminele bendes, ook veel low-levelcybercriminelen actief zijn. Het stereotype van de zolderkamerhacker klopt in veel gevallen nog best wel vrij accuraat. Het zijn vaak individuen die activiteiten uitvoeren voor roem en erkenning, meer dan voor financieel gewin. Het idee in de sector leeft dat een strategie waarbij aanbieders van illegaal aangeboden auteursrechtelijk beschermd materiaal, video, geluid et cetera, benaderd en vervolgd zouden moeten worden als effectief afschrikmiddel voor het grote volume aan aanbieders dat gestolen informatie, slachtofferdata, aanbiedt. De grote spelers zullen hier waarschijnlijk niet of beperkt door worden beïnvloed. Maar als je die community's verstoort, kan je toch best een volume aan darkwebplatforms inperken door de populariteit te verminderen? Hoe kijkt de minister van Justitie daartegen aan? Herkent ook de politie dit beeld en lukt het om deze community's effectief te verstoren?

Voorzitter. Dat was het van mijn kant. Dank u wel.

De **voorzitter**:
Heel hartelijk dank, heer Six Dijkstra, voor uw bijdrage. Ik zie geen verdere interrupties. Dan geef ik het woord aan mevrouw Michon-Derkzen namens de Volkspartij voor Vrijheid en Democratie voor haar eerste termijn.

Mevrouw **Michon-Derkzen** (VVD):
Dank, voorzitter. Ik ben blij dat er intussen nog twee leden zijn aangeschoven, want het is een enorm belangrijk onderwerp. Het is eigenlijk onbegrijpelijk dat er geen enorme politieke aandacht voor is, want dit onderwerp raakt ons allemaal. Het raakt mensen thuis, het raakt onze bedrijven en het kan ook ons land raken. Het gaat eigenlijk om het vertrouwen dat wij in onze ICT-systemen hebben. Het gaat om weerbaarheid. Het gaat om onze cyberveiligheid, maar ook om de rapid response op alle niveaus. ICT-uitval of

een cyberaanval — dat zien we helaas langskomen — heeft direct impact op onze manier van leven. Ik ben dan ook blij met alle documentatie die we van het kabinet hebben gekregen, maar tegelijkertijd is het wel veel papier. Kunnen we deze informatie wat meer naar resultaten toe schrijven: wanneer zijn we dan tevreden, wat willen we nou bereiken en waar staan we dan? Ik vraag dit ook in het kader van de oproep van de minister van JenV met zijn collega van Defensie over de hybride dreigingen van statelijke actoren. Daar zit evident ook een deel in wat over de cybersecuritystrategie gaat. Althans, dat mag ik hopen. Hoe ziet dan die uitvoering eruit? Past dat dan binnen de bestaande strategie of krijgt dat dan een uitbreiding?

De cyberweerbaarheid van bedrijven is natuurlijk een belangrijk aandachtspunt; ik kijk even naar de minister van Economische Zaken. We hebben er ook in het verleden vaker aandacht voor gevraagd. De Cyber Security Raad heeft het over die kloof. Die heeft het natuurlijk vooral over kleine bedrijven die het ingewikkeld vinden om die weerbaarheid op orde te krijgen. Hoe zit dat nou? Wat doen we eraan om ook die kleine bedrijven te beschermen? In dat kader wil ik ook vragen of die kleine maar ook mkb-bedrijven het nieuwe NCSC kunnen vinden, waar ook het DTC onderdeel van is geworden. Hebben zij nog een zichtbaar loket? Weten ze dat te vinden? Ik denk dat de minister gaat zeggen: ja hoor, dat weten ze te vinden. Ik wil graag dat hij dat verifieert bij de bedrijven waar het om gaat, want we moeten dat loket openhouden.

Hetzelfde vraag ik aan de minister van Economische Zaken over zijn agenda Cybersecurity Technologies. Is die nu ook onderdeel van de cybersecuritystrategie, van die brede strategie? Hoe past die daarin?

Ik ben het zeer eens met de woorden van collega Six Dijkstra dat er in bestuurlijk Nederland echt nog een wereld te winnen is als het gaat om de bewustwording over cyberveiligheid. We hebben die oefeningen, ISIDOOR IV. Hebben bestuurders daar een actieve rol in? Kunnen we veiligheidsregio's ook een rol geven in die oefeningen? Eigenlijk zou ik het liefst gewoon het land, wij met z'n allen, een rol willen geven in zo'n oefening. Ik denk oprecht dat het voor velen in ons land in ons dagelijks leven een ver-van-je-bedshow is, terwijl we er echt meer beeld bij moeten hebben: wat gebeurt er dan? Stel dat er even van alles uitvalt, zoals een bank, een publieke instelling zoals een gemeentelijke basisadministratie, een stoplicht en noem maar op. Hoe pakken we dan die rapid response aan? Er is per definitie schaarste aan cybersecurityexpertise. Waar zetten we die dan in? Is het denkbaar dat je publieke expertise inzet voor een private sector, omdat die nou eenmaal een hogere prioriteit heeft? Is dat ook besproken? Wordt daarover gesproken en zit er een soort systeem in wie als eerste de schaarse capaciteit krijgt? Want dat die capaciteit schaars is, is evident.

In dat kader wil ik ook graag naar de sector zelf. De hele cybersecuritydienstverlening is natuurlijk booming business. Ik vind het heel goed dat zij ook zelf werken aan kwaliteitsstandaarden. Hoe weet je nou of je met een bedrijf, met een dienstverlener samenwerkt die aan de kwaliteitsnormen voldoet? Ik begreep dat er voor pentesten nu een keurmerk is, maar komen er ook voor andere diensten in de sector zelf kwaliteitsstandaarden die leiden tot een keurmerk? Hebben we er als overheid een goed beeld van of die keurmerken en die kwaliteitsstandaarden inderdaad op het goede niveau zitten? Ik denk dat dat essentieel is, juist voor de schaarse capaciteit die we hebben in de cybersecurity. Ik zou ook hopen, zeg ik weer richting de minister van Economische Zaken, dat we dan dat soort keurmerken ook als een eis in onze Europese

aanbestedingen hebben, zodat wij als overheid zaken doen met die bedrijven die wij van goede kwaliteit vinden.

Ik heb vijf minuten, voorzitter.

De **voorzitter**:
Nog tien seconden.

Mevrouw **Michon-Derkzen** (VVD):
U kijkt mij heel indringend aan, maar ik heb nog vijftien seconden. Tien? Nou, oké.

Dan als laatste punt NIS2. Daar wilde ik nog van alles over zeggen, maar dat zal ik dan inperken. Ik wil graag nog wel van dit kabinet weten of wij voor ons zien hoe we de informatie-uitwisseling tussen private en publieke partners gaan ontwikkelen. Is Cyclotron, dat we nu in de steigers hebben staan, inderdaad het model dat het kabinet voor zich ziet? Wat kunnen we leren van het project Melissa? Dat ging over ransomware, maar gebruiken we het ook voor de doorontwikkeling van Cyclotron? Al die private bedrijven willen natuurlijk weten: hoe krijg ik die informatie, hoe kan ik dit goed doen?

Dank u wel, voorzitter.

De **voorzitter**:
Dank voor uw bijdrage. U heeft een interruptie van de heer Six Dijkstra, Nieuw Sociaal Contract.

De heer **Six Dijkstra** (NSC):
Aangezien ik verwacht dat het vandaag geen nachtwerk wordt, wil ik mevrouw Michon vragen welke vragen zij nog over NIS2 wilde stellen om haar toch even de ruimte te geven.

Mevrouw **Michon-Derkzen** (VVD):
Dat is zo aardig! Heb ik zelf niet een keer verteld hoe je dat moet doen als Kamerlid? Voorzitter, ik zit ook weleens waar u zit. Het is roeien met de riemen die je hebt. Heel aardig van meneer Six Dijkstra.

Nu we de implementatietermijn van NIS2 niet gaan halen, zou ik graag willen weten wat het kabinet doet om toch al die bedrijven voor te bereiden op hetgeen komen gaat. Wat kunnen zij dit kalenderjaar verwachten? Hoe zorgt het kabinet ervoor dat ze voldoen aan de eisen uit de NIS2-richtlijn, maar voorkomt het tegelijkertijd dat die bedrijven allerlei onnodige bureaucratie ... Ja, er komt iets van bureaucratie bij kijken, maar hoe houden we dat nou binnen de perken? Ik zou het interessant vinden om dat te weten. Ik denk ook dat vooral een heel aantal bedrijven die dit volgen het graag willen weten.

Tot slot, met dank aan de heer Six Dijkstra, zou ik een reactie van het kabinet willen op de roep om wetgeving voor de aanpak van bankhelpdeskfraude. Dat zagen we deze week in het nieuws. Er is aanpassing van telecomwetgeving nodig; ik kijk naar de minister van Economische Zaken. Zoals ik mijn bijdrage begon: van de keukentafel tot aan het land. Het zit overal. Ik denk dat we moeten beginnen met perspectief geven voor ... Nou ja, we moeten het eigenlijk allebei doen, maar in ieder geval aan die keukentafel.

Dit zou een goede oplossing kunnen zijn voor de aanpak van bankhelpdeskfraude.

Dank u wel, voorzitter.

De **voorzitter**:
Heel hartelijk dank voor uw bijdrage en de heer Six Dijkstra voor zijn creatieve oplossing. Dan zie ik geen verdere interrupties. O jawel, een interruptie van mevrouw Kathmann, GroenLinks-PvdA.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik kan me eigenlijk heel goed vinden in het pleidooi van mevrouw Michon-Derkzen van de VVD over veel papier. We moeten concreet met de bal op de uitvoering, want de urgentie is ongelofelijk groot. Mevrouw Michon-Derkzen sprak ook over kleinere bedrijven, het mkb. Wat vindt zij van het voorstel uit de cybersecurity zelf dat we op zo veel mogelijk werkvloeren digitale hulpverleners krijgen, eigenlijk het eerste aanspreekpunt bij een cyberongeval, zodat er dan zo snel mogelijk iets aan gedaan kan worden? Dan gaat het ons misschien miljarden minder kosten.

Mevrouw **Michon-Derkzen** (VVD):
Als je een bedrijf hebt, zorg je natuurlijk dat je bedrijf overeind blijft. Dat lijkt me een beetje de basis voor iedereen die een bedrijf runt. In deze tijd is het dus nodig dat je ook je cybersecurity op orde hebt en dat als je wordt aangevallen, je die respons ... Het heet elke keer "rapid response"; ik weet helemaal niet hoe we dat in het Nederlands zeggen. Er wordt gezegd "snelle reactie", maar dat is weer iets heel anders. Maar goed, het is in ieder geval nodig dat je daar snel en effectief op reageert. Ik vind dat gewoon onderdeel van de bedrijfsvoering van een bedrijf. Daarom zie je dat de hele cybersecuritysector zelf ook booming is, want er is veel vraag naar die expertise. Ik vind dat de overheid moet helpen om kaders te stellen. Wat is er nodig? Wanneer moet je waaraan denken? Wat zijn straks de richtlijnen, de eisen vanuit NIS2? Dat zijn allemaal hele belangrijke zaken zodat een bedrijf zich daar goed op kan voorbereiden. Dat is per definitie publiek-private samenwerking, maar een bedrijf zelf zal natuurlijk zijn eigen cybersecurity op orde moeten hebben. Dat is gewoon onderdeel van je bedrijfsvoering.

De **voorzitter**:
Dan zie ik geen vervolgvraag van mevrouw Kathmann. O, toch nog een vervolgvraag.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Als we dit op papier zouden zetten, zouden we weer heel veel papier hebben, weinig concreet en niet de bal op de uitvoering. Er is uit de cybersecuritysector een voorstel gekomen om, omdat het toch vaak in menselijk handelen zit als het fout gaat, bedrijven er zo veel mogelijk op te attenderen: zorg in ieder geval dat dat aanspreekpunt er is, dat je die rapid response hebt. Die persoon, die digitale hulpverlener, weet precies wat die wanneer, en dus snel, moet doen. Het is niet zoals bij een echte bedrijfshulpverlener dat je er allerlei cursussen voor nodig hebt. Stel die persoon gewoon aan, laagdrempelig, of een persoon die weet welke externe je moet bellen, ook tijdens de vrijdagmiddagborrel, zodat er niet een heel weekend overheen gaat. Dus heel concreet is de vraag: vindt de VVD dat een goed voorstel of niet?

De **voorzitter**:
Het woord is aan mevrouw Michon-Derkzen. Moet het onder de KAM-coördinator

vallen?

Mevrouw **Michon-Derkzen** (VVD):
Ik denk dat we hier het ideologische verschil tussen mevrouw Kathmann en mijn partij bloot gaan leggen. Ik vind het heel logisch dat er iemand is die dit doet en dan gaat mevrouw Kathmann zeggen "dan moet je dat vastleggen en dan moeten we het misschien registeren of doen", zoals we allerlei dingen vastleggen voor bedrijven. Het punt dat ik net inbracht, is dat een goede aanpak van cybersecurity in een bedrijf onderdeel is van de normale bedrijfsvoering. Daar hoort ook bij dat je ervoor zorgt dat je ofwel met mensen in huis ofwel met een dienstverlener onder contract reageert als dat nodig is. Dus als je dat niet doet als bedrijf, dan neem je daarmee zelf ook het risico om zwaar aangevallen te worden met alle gevolgen van dien. We zijn het dus eens dat het belangrijk is voor een bedrijf, maar mijn stelling is dat een bedrijf, de baas van een bedrijf, dat altijd zelf zal regelen. Ik hoor mevrouw Kathmann zeggen: vindt u dat dat niet geregeld moet worden? Ja, dat regelt de baas van die onderneming zelf, want daarom heeft die een onderneming. Dat is de kern van zijn bestaan. Ik denk dat ik daar zomaar anders over denk dan mevrouw Kathmann.

De **voorzitter**:
Dan zie ik nog een laatste vervolgvraag van mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ja, want het nodigde wel weer uit om iets te zeggen. Volgens was mijn bijzin juist om helemaal niks vast te leggen, maar vooral om een campagne te starten om bedrijven hierop te attenderen. Want heel veel mkb'ers willen heel, heel graag aan de slag. Het zijn allemaal ondernemers en die weten heel, heel goed hoeveel geld het ze kan kosten als ze gepakt worden: gemiddeld 2 ton per bedrijf. Inmiddels — mevrouw Michon-Derkzen zei het zelf ook al — is er een hele markt ontstaan in die cybersecuritywereld en is cyberveilig worden en zijn voor heel mkb'ers ongelofelijk duur, los van dat het soms ook ingewikkeld is. Laten we dan in ieder geval een campagne starten en zeggen: "Hé, zorg nou voor die persoon. Dan heb je die rapid response. Dan heb je in ieder geval een eerste laagdrempelige inzet. Daar hoef je niet een nieuw iemand aan te nemen. Dat is een beetje waar je de basis op orde kan krijgen. Daar hoef je niet honderden of duizenden of weet ik het wat euro's tegenaan te smijten. Het is gewoon een hulpmiddel." Wij lezen namelijk ook in alle papieren die we toegestuurd krijgen dat het voor heel veel mkb'ers in Nederland best ingewikkeld is om de boel op orde te krijgen, omdat het gewoon heel veel investeringen vraagt. Dus minder investeringen en toch veiligheid: dat lijkt mij een heel fijne manier om Nederland gewoon weer cyberveilig te krijgen.

Mevrouw **Michon-Derkzen** (VVD):
Ik heb in mijn bijdrage ook gevraagd naar die kloof als het gaat om cyberweerbaarheid. Het begint met bewustwording. Dat ben ik zeer met mevrouw Kathmann eens. Kleine bedrijven moeten echt weten met welke gevaren en met welke risico's ze te maken hebben. Ik lees ook in al die stukken dat er een kloof is. Daar vraag ik een reactie van het kabinet op en ook op hoe we die dichten. Dus bewustwording is één ding en als je weet wat je te doen staat als bedrijf, dan moet je dat doen. Dan moet je dat doen met iemand in dienst of met een contract met een dienstverlener. Daar treed ik niet in.

De **voorzitter**:
Heel hartelijk dank voor uw bijdrage. Dan zijn we toch bij mevrouw Koekkoek, die

namens Volt haar bijdrage in eerste termijn zal doen.

Mevrouw **Koekkoek** (Volt):
Dank, voorzitter. We hebben de afgelopen weken al veel met elkaar besproken deze commissie — we hebben een soort sprint gehad als het gaat over debatten — maar ik ben toch blij dat we hier vandaag weer zijn, want er is, zoals collega Michon ook al aangaf, een hele hoop aan de hand en dat raakt ons allemaal. We zijn al een tijdje op het punt dat we de problemen in de fysieke wereld niet los kunnen zien van de onlinewereld. We kunnen de impact van wat er in de VS gebeurt en de ontwikkelingen op het gebied van AI en andere technologieën in China ook niet los zien van wat we vandaag bespreken. Digitale politiek is geopolitiek en dat beïnvloedt onze onlineveiligheid en cybersecurity. Daarom heb ik een aantal vragen over de volgende onderwerpen: hybride dreigingen, vitale infrastructuur en cybersecurity en Europa.

Voorzitter. Eerst de militaire dreiging en paraatheid. Het ministerie van Justitie en Veiligheid is daar samen met de minister van Defensie verantwoordelijk voor. We hebben in oktober een brief ontvangen waarin het kabinet aangeeft dat het druk bezig is met het versterken en het maken van beleid, maar het blijft in ieder geval voor mij onduidelijk waar het precies op toeziet. Ik wil dus vragen of de minister kan toelichten hoe de aanpak van desinformatie, digitale weerbaarheid, cyberveiligheid en hybride dreigingen de komende maanden vorm zal krijgen. Door het op te nemen op zo'n brede lijst van onderwerpen, kunnen de precisie en de verantwoordelijkheid naar de achtergrond verschuiven. Daar hoor ik graag concretere acties op. Komt er bijvoorbeeld nieuw beleid, wordt het opgenomen in de lopende Nederlandse Cyber Securitystrategie, de NLCS, of vinden we het terug in de Digitaliseringsstrategie van de staatssecretaris? En vanuit welke begroting wordt dit bekostigd, zou ik nog willen vragen.

Er bestaat een grote behoefte in de Nederlandse samenleving om meer informatie te krijgen over hybride conflictvoering als gevolg van de oorlog in Oekraïne. Ik denk ook dat een groot deel van die dreiging niet per se bekend is bij de Nederlandse bevolking in het algemeen. Daarom wil ik aan het kabinet vragen wat zij gaan doen om burgers beter te betrekken bij de hybride conflictvoering en vooral hoe ze gaan ondersteunen in de weerbaarheid en het meer geïnformeerd maken van mensen.

Eerder diende mijn fractiegenoot Laurens Dassen twee moties in. Eentje ging over het vergroten van de productiecapaciteit op het gebied van elektronische oorlogsvoering en de inzet van het Defensiefonds daarvoor. Een andere ging over inspanningen om de strategische inlichtingencapaciteit van Europa te vergroten. Die eerste is aangenomen en ik ben benieuwd welke rol deze minister gaan spelen bij het uitvoeren van deze motie. Of ligt dit dan volledig bij Defensie? Als het antwoord daarop ja is, dan ben ik wel benieuwd waarom. Ik denk namelijk dat dit veel raakvlakken heeft. De tweede motie, over het vergroten van de strategische inlichtingencapaciteit in Europees verband, is niet aangenomen, maar ik wil toch vragen aan deze ministers hoe zij daarover denken, want het betreft ook hun beleidsterreinen.

Voorzitter. Een ander onderwerp, waar wij het vorige week ook over hebben gehad, is kwantumveiligheid. Van de staatssecretaris kregen wij het beeld dat de overheid wel degelijk bezig is met het kwantumbestendig maken van onze vitale processen, maar ik wil daar wel nog graag op doorvragen. Welke maatregelen neemt het kabinet om ervoor te zorgen dat de cybersecurity van Nederland en ook Nederlandse bedrijven

kwantumbestendig worden en welk concreet tijdpad is daaraan verbonden? Het ligt natuurlijk in de toekomst, maar eigenlijk zouden we nu ook al richting bedrijven die stappen moeten zetten.

Dan een ander onderwerp waar de laatste tijd veel aandacht voor is: sabotage van vitale infrastructuur. Eerst waren het met name gasleidingen die de interesse hadden van buitenlandse mogendheden om te saboteren en nu zien we de aandacht langzaam verschuiven naar internetverbindingen, zoals onlangs bij de glasvezelkabel in de Oostzee. Kunnen de ministers uitleggen of toelichten wat zij doen om risico's te mitigeren? In de Oostzee is nu een NAVO-missie gestart. Is dit iets waar we ook in het Nederlandse deel van de Noordzee beducht voor zouden moeten zijn?

Dan Europa. Dat heeft zoals altijd niet stilgezeten en dat is maar goed ook. De afgelopen jaren is gewerkt aan een heel pakket Europese wetgeving om cybersecurity beter in te bedden in onze economie en ook in onze samenleving. Ook vanuit Nederland is gewerkt aan aanvullende wetgeving. Dan komt er een heel rijtje afkortingen. Ik zal proberen om ze helemaal uit te spreken. Het gaat om de NIS2, waar net ook al wat over werd gezegd, de SER-richtlijn, de Cyber Resilience Act, de DORA en de Wet bevordering digitale weerbaarheid bedrijven. Met het oog op de tijd gebruik ik even alleen de afkortingen. Ik wil de vraag stellen hoe klaar Nederland al is om deze wetgeving te implementeren. Op sommige implementatietrajecten zit vertraging. Daarom wil ik dezelfde vraag stellen als collega Michon, namelijk wat we nu al wel doen en hoe we daar ook bedrijven in meenemen.

Vanuit de mkb-sector en dan met name de kleine en micro-ondernemingen wordt aangegeven dat het totale pakket aan maatregelen zorgt voor grote administratieve druk. Bedrijven willen heel graag voldoen aan die wet- en regelgeving, maar daarin is wel extra ondersteuning nodig. Ik zie u kijken, voorzitter. Ik wil de vraag stellen welke impact het kabinet verwacht voor het mkb. Wat doen de ministers om hen extra te ondersteunen? En wat wordt er gedaan voor start-ups in belangrijke sectoren? Want dat is nog net weer een ander verhaal dan het mkb.

Dank, voorzitter.

De **voorzitter**:
Heel hartelijk dank voor uw bijdrage, mevrouw Koekkoek. Keurig binnen de tijd. Ik zie geen interrupties. U had zelfs nog elf seconden over. Sorry, ik wist niet dat ik streng keek. Excuses daarvoor. Nou, dan mag ik het woord geven aan mevrouw Kathmann, die haar inbreng zal doen namens GroenLinks-PvdA.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dank, voorzitter. Als het over cybersecurity gaat, moet ik hier eigenlijk altijd een beetje denken aan de film Groundhog Day. Ik weet niet of mensen die film kennen, maar die gaat eigenlijk over een dag die zich de hele tijd herhaalt en die elke keer weer begint met "It's Groundhog Day". We horen elke dag de waarschuwingen dat de cybersecurity van Nederland niet op orde is. We horen ook elke dag dezelfde boodschap "de digitale dreiging is groot" en we horen elke dag "onze weerbaarheid is onvoldoende". Ondertussen verliezen we miljarden euro's per jaar, omdat cybersecurity voor heel veel organisaties duur is, ingewikkeld is en omdat ze niet de juiste mensen kunnen vinden. Die cyberweerbaarheidskloof lijkt maar niet kleiner te worden, terwijl kwaadwillenden

altijd achter de zwakste schakel aangaan. Kan de minister aangeven welke maatregelen hij heeft getroffen om de cyberweerbaarheidskloof te dichten? Acht de minister dit voldoende? Welke doelen voor het dichten van de cyberweerbaarheidskloof stelt de minister zich, en denkt hij dat hij met deze maatregelen die doelen gaat halen?

Onze fractie heeft eerder opgeroepen tot het publiceren van een lijst van betrouwbare gratis opensourcecybersecuritysoftware die Nederlanders kunnen gebruiken om hun cyberveiligheid te verbeteren. Wat vindt de minister hiervan? Hoe trekken deze ministers gezamenlijk op, ook met andere ministers, om een heel stevige agenda neer te leggen als het gaat over het opleiden van personeel? Dan heb ik het dus eigenlijk over een soort deltaplan voor cyberbanen en onderwijs.

Dan wil ik er nogmaals op wijzen dat honderd procent cybersecurity niet bestaat. De vraag is niet of, maar wanneer het misgaat. Hierbij is heel vaak de mens de zwakste schakel. Dat is natuurlijk heel logisch, want fouten maken is gewoon menselijk. We worden allemaal een keer de persoon die op die link klikt. Dat geldt ook voor mij en ik schaam me dan ook en denk dan: o nee, ik ben erin getrapt. Dat gevoel snap ik dus ongelofelijk goed. Het is zo belangrijk dat we afkomen van dat taboe, want dat zou al heel veel ellende schelen. Op zo'n moment wil je weten, zeker als je bij een bedrijf werkt, dat een collega je kan helpen en precies weet wat de eerste stappen zijn, een soort basishulpverlener voor ICT, een digitale hulpverlener oftewel een dhv'er. GroenLinks-Partij van de Arbeid wil nog een keer de aandacht voor meer dhv'ers bij bedrijven en organisaties. Daartoe is een motie van mij aangenomen en daarom wil ik de volgende vragen stellen.

De **voorzitter**:
Voordat u uw vragen stelt, is er een interruptie van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Ik vind het mooi — lof daarvoor — dat mevrouw Kathmann zegt: het kan mij ook overkomen. Het kan mij ook overkomen. Het gebeurt ook bij heel veel mensen thuis en die schamen zich allemaal kapot. De aangiftegetallen van onlinefraude zijn daarom bijvoorbeeld enorm laag. Ook de schadeloosstelling is enorm moeilijk en dat komt onder andere doordat er grote barrières zijn bij het delen van informatie, bijvoorbeeld tussen private en publieke organisaties. We hebben de Fraudehelpdesk en daar is dit echt hét punt, want die krijgt enorm veel dingen binnen. Maar de helpdesk mag niets zeggen. Ze mag niet eens aangeven: let op, dit is wat er gebeurt. Afgelopen november heb ik daarvan bij de begroting een punt gemaakt, ook om ervoor te zorgen dat we met elkaar die barrières slechten en dat die informatie wel kan worden gedeeld, juist om die gedupeerden te helpen. Hoe kijkt mevrouw Kathmann daartegen aan?

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dat is een goede vraag. Toen mevrouw Michon-Derkzen klaar was met haar bijdrage, zei ik al dat ik me daar heel goed in kan vinden. Dat geldt zeker voor wat betreft haar vraag of mkb'ers de juiste weg wel weten te vinden. En als mkb'ers de juiste weg weten te vinden, kunnen ze dan hulp krijgen of zitten daar dingen in de weg? Op dit moment doet de commissie Digitale Zaken op eigenlijk elk terrein exercities, dus niet alleen op dit terrein, maar ook bij bedrijven die financieringsrisico's inventariseren of bij het onderwijs. Wat zit er nou in de weg en welke regel is het? Welke juridische grondslag moeten we eigenlijk gaan regelen om het voor elkaar te krijgen? Dus dat steun ik echt van harte.

De **voorzitter**:
Een vervolgvraag van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Dat vind ik heel goed om te horen, want het is juist vaak zo dat we elkaar op de analyse weten te vinden, maar niet op de oplossingen. Als het gaat om het delen van informatie, wordt het vinden van oplossingen veel ingewikkelder. Ik kom mevrouw Kathmann ook niet in elk debat tegen. Dat wil ik ook maar gezegd hebben; vaak zijn het haar collega's. Maar haar partij is dan wel vaak de partij waarmee ik behoorlijk in de clinch lig over de noodzakelijke maatregelen. Dat is namelijk heel vaak het beslechten van die barrières in de informatiedeling. Ik neem dit dan maar aan als een constructieve reactie van mevrouw Kathmann en haar partij op mijn vraag om informatie waar nodig te delen tussen publieke en private partners. Zo kunnen we namelijk echt met elkaar kijken hoe we het voor elkaar kunnen krijgen om gedupeerden beter en sneller te helpen.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Hier wil ik nog wel op reageren. Het is volgens mij mijn hele missie, want er gaat geen cybersecuritydebat voorbij of ik zeg dit! Het is mooi dat ik daar nu ook een moment voor heb. Ik wil echt af van die schijntegenstelling tussen privacy en veiligheid. Privacy is veiligheid. Ik zei net al tegen mevrouw Michon-Derkzen, toen zij haar bijdrage begon met "we moeten hier nu eindelijk eens concreet worden naar de uitvoering", dat wij bezig zijn met een exercitie om dit voor elkaar te krijgen. Ik kom uit Rotterdam en ik ben nogal van "geen woorden, maar daden". Ik lig hier dus helemaal niet in de clinch. Ik ben hier gewoon op dagelijkse basis mee bezig. Ik hoop dat we hier snel stappen in kunnen zetten.

Het is alleen wel waar dat als we burgers willen beschermen, we vaker zorgvuldig een juridische grondslag moeten regelen. Ik heb begrepen dat dit heel vaak van de zijde van het kabinet uitblijft, omdat we soms ook niet weten waar het probleem zit. Maar als Tweede Kamer zijn wij natuurlijk ook medewetgever. Wij moeten ons dat natuurlijk ook aantrekken, maar initiatieven van onze zijde blijven desondanks uit. En dat is nou precies wat ik aan het oppakken ben. Dus mevrouw Michon-Derkzen is van harte uitgenodigd om zich daarbij aan te sluiten.

De **voorzitter**:
Continueert u uw betoog, mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik heb een aantal vragen aan de minister over de motie en over de digitale hulpverlener. Kan de minister aangeven op welke manier hij bedrijven heeft geïnformeerd over de mogelijkheid om dhv'ers aan te stellen via het Digital Trust Center? Kan de minister enig inzicht geven in hoeveel bedrijven een dhv'er hebben aangesteld? Is de minister tevreden met dat aantal en wat wil de minister allemaal nog meer doen om dat aantal omhoog te krijgen? Zijn er binnen overheidsorganisaties ook al dhv'ers aangesteld? Welke zijn dat en gaat de minister zich inspannen om dit aantal omhoog te krijgen? Bij cybersecurityincidenten is het belangrijk dat er zo snel mogelijk gereageerd wordt en daarom vind ik die dhv'er ook zo ongelofelijk belangrijk.

Maar gelukkig zijn er ook heel veel goede voorbeelden van hoe je met cyberincidenten

kunt omgaan. Ik vind het bijvoorbeeld echt een pluim waard hoe die centralisten van de 112-meldkamers doorwerken. Er zijn daar een aantal storingen geweest, maar dat gaat, gewoon hop, analoog door. Die hebben echt heel goed nagedacht over hun plan B. Maar dat moeten veel meer organisaties gaan doen.

GroenLinks-Partij van de Arbeid vindt dat in ieder geval essentiële organisaties zoals gemeenten, ziekenhuizen en universiteiten allemaal een plan B moeten hebben, een plan om zo snel mogelijk, binnen 48 uur, te kunnen overstappen op analoge manieren om essentiële dienstverlening doorgang te kunnen laten vinden, terwijl de professionals hard werken aan het herstel van systemen en back-ups. Het kabinet is zo vriendelijk geweest om mijn motie die dit vraagt, over te nemen, maar dan verwacht ik wel actie. Hoe gaat dit kabinet die overgenomen motie uitvoeren en bij welke sectoren gaat het kabinet helpen om een 48 uursplan te maken?

Tot slot, voorzitter, want anders gaat u heel streng kijken. Digitalisering en kennis van cybersecurity zijn essentieel voor elke organisatie, van groot tot klein. We verwachten van ondernemers en bestuurders dat ze kennis hebben van financiële en juridische zaken. Het is nu 2025 en daarom wil ik daaraan toevoegen dat ze ook kennis moeten hebben van digitale zaken. De heer Six Dijkstra zei er ook al wat over. Naast een financieel en sociaal jaarverslag zou eigenlijk elke grote organisatie voortaan een cyberjaarverslag moeten overwegen. Daarin ga je in op de digitale stand van zaken zoals het aantal cybersecurityincidenten dat heeft plaatsgevonden en de trainingen op de werkvloer. Maar je gaat daarin dan ook in op bijvoorbeeld migraties naar nieuwe clouddiensten.

Ik ben blij dat daar, al is het kort, in de Voortgangsrapportage Nederlandse Cybersecuritystrategie 2024 ook al bij stil wordt gestaan. Maar ik zou iets uitgebreider van de minister willen weten wat hij vindt van het idee van een cyberjaarverslag. Hoe gaat hij hiermee aan de slag? En kunnen we dit breed, maar in ieder geval in overheidsland, uitrollen?

Heb ik nog even, voorzitter? Ja? Maar echt als allerlaatste een pluim voor de politie. Ik denk dat niemand het in Nederland heeft gemist dat de politie rondom de feestdagen en Black Friday heel succesvol heeft gewaarschuwd voor oplichting online. In die periode slaan cybercriminelen ook vaker toe. Hoe gaat de minister ervoor zorgen dat de politie zulke acties kan uitbreiden, voortzetten en noem maar op? Want dit was echt een daverend succes. Een grote pluim daarvoor!

De **voorzitter**:
Heel hartelijk dank voor uw bijdrage. Ik zie dat er verder geen interrupties zijn. Ik draag heel even het voorzitterschap over aan de heer Six Dijkstra, want dan kan ik mijn pet als voorzitter afzetten om mijn bijdrage te doen.

Voorzitter: Six Dijkstra

De **voorzitter**:
Ik geef bij dezen het woord aan de heer Valize, die namens de PVV het woord zal voeren.

De heer **Valize** (PVV):

Voorzitter, dank voor het woord. Met het thema onlineveiligheid en cybersecurity richt de commissie Digitale Zaken zich op de veiligheid van digitale technologie en de beveiliging van informatie. We gaan als DiZa dus niet over de invulling van de taken van andere commissies. Dat gezegd hebbende mijn volgende bijdrage. Vijf minuten is wat kort en ik ga daarom een beetje van de hak op de tak.

Voorzitter. Het doet de fractie van de PVV deugd dat de integratie van het Nationaal Cyber Security Centrum, het NCSC, het Digital Trust Center, DTC, en het Computer Security Incident Response Team voor digitale dienstverleners, het CSIRT-DSP, op schema ligt, om maar eens met iets positiefs te beginnen. Echter, hoe borgt de minister dat dit niet leidt tot een afname van de laagdrempelige ondersteuning van het mkb? Dat is een vraag die de VVD ook al stelde.

Dan de voortgang bij de Nederlandse Cybersecuritystrategie. Opvallend is dat in de beslisnota bij de Kamerbrief Cybersecuritybeeld Nederland 2024 en in de voortgang Nederlandse Cybersecuritystrategie gesproken wordt over het feit dat er geen wijzigingen aan het actieplan noodzakelijk worden geacht, terwijl er juist niet alleen extra wordt ingezet op de dreiging van landen met een offensief cyberprogramma, maar ook op de doorontwikkeling van het Cyberweerbaarheidsnetwerk. Immers, het kabinet geeft aan te willen inzetten op de bestrijding van digitale criminaliteit. En dat is ook logisch gelet op alle activiteiten van de afgelopen twaalf maanden.

Voorzitter. In het vorige debat over dit thema op 11 april 2024 noemde ik het rapport van Dialogic. Hierin werd een beraming opgenomen om het programma van het actieplan, alle 136 actiepunten dus, uit te voeren tot en met 2028. Er zou in totaal 568 miljoen euro benodigd zijn. Zijn de genoemde budgetten nog steeds toereikend, want met het verlengen van de focus kan het niet anders dan dat dit budgettaire gevolgen heeft? Hoe zit het? Loopt deze nog gelijk aan de oorspronkelijke raming? En ook wil de PVV weten of de focus op weerbaarheid tegen militaire en hybride dreigingen binnen de NLCS lopend of nieuw beleid betreft. En vanuit welke begroting wordt dit bekostigd? Een vraag die de collega van Volt ook stelde.

Voorzitter. Dan het Samenhangend Inspectiebeeld cybersecurity vitale processen 2024. Dat zou betrokken worden bij de Voortgangsrapportage Nederlandse Cybersecuritystrategie, maar in de voorgangsbrief wordt niet toegelicht hoe het kabinet de uitkomsten uit het inspectiebeeld erbij betrekt. Hoe gaat dit erbij betrokken worden?

Dan nog een ander onderwerp: het CE-keurmerk. Dat acht ik toch wel belangrijk, immers ... Als ik daarmee buiten de tijd ga, dan is dat maar zo, voorzitter. Het staat immers niet op de agenda van vandaag, maar het behoort hier wel besproken te worden. Op 11 april 2024 spraken we ook over onlineveiligheid en cybersecurity. Tijdens dit commissiedebat spraken wij onder andere over de Cyber Resilience Act en daarbij bracht de PVV nog het CE-keurmerk aan.

Ten behoeve van de veilige aanschaf van producten dient de burger op te letten dat het artikel van aankoop voorzien is van een dergelijk keurmerk. Als dit CE-keurmerk erop staat, dan is het goed. We hebben toen aangekaart dat er twee CE-logo's bestaan. De lettertypes zijn identiek en het enige verschil is een spatie. De reactie van de toenmalige minister luidde als volgt. Ik citeer, dus zet de klok maar even stil want dit behoort niet van mijn spreektijd af te gaan. "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." Einde citaat.

Voorzitter. We zijn nu bijna een jaar verder. Er is geen brief, geen terugkoppeling. Er is niets! Deze toezegging is overigens ook niet als toezegging genoteerd. Daarom wil ik nu toch wel een keiharde toezegging, want het gaat hier, verdorie, om de nationale veiligheid! Desnoods kom ik met een motie, want dit kan niet blijven liggen.

In de Voortgangsrapportage Nederlandse Cybersecuritystrategie 2024 wordt op pagina 18 gesproken over de motie-Rajkowski en het keurmerk voor ICT-dienstverleners ten behoeve van het mkb. Laat me raden. CE? Of wordt deze wel echt onderscheidend? Ik begin me toch echt zorgen te maken, want we gooien of bakken met geld weg om schijnveiligheid hoog te houden of we komen met iets concreets dat ook daadwerkelijk werkt.

Daarmee, voorzitter, kom ik aan het einde van mijn betoog.

De **voorzitter**:
Dank u wel, meneer Valize. Met vier minuten en achttien seconden bent u ruim binnen de tijd gebleven, maar u heeft nog een interruptie van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
De heer Valize noemde de motie van mijn collega Rajkowski. Zij heeft gepleit voor een keurmerk, zodat bedrijven die cybersecuritydienstverlening inhuren weten met wie ze te maken hebben. Ik wil het even scherp hebben. Ik ben toen niet bij die discussie geweest, maar pleit de heer Valize ook voor het doorontwikkelen van een dergelijk keurmerk, zoals we dat ook hebben voor de pentest?

De heer **Valize** (PVV):
Dank voor deze vraag. Wij hebben er destijds voor gepleit om dat niet te doen, omdat een extra keurmerk weer extra regeldruk voor bedrijven betekent. Als het een heel goed voorstel is dat weinig tot geen administratieve lasten met zich meebrengt, willen we erover nadenken, maar dan moet er wel eerst een voorstel liggen. Ik vraag me wel af of we daarmee schijnveiligheid creëren of dat het daadwerkelijk iets gaat opleveren. Vandaar ook mijn vraag aan de minister.

De **voorzitter**:
Een vervolgvraag van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Natuurlijk zal niemand pleiten voor schijnveiligheid. Dat zult u van mij ook niet horen. Maar de vraag is wel of de kwaliteit van de dienst die je inhuurt, op orde is. Je huurt immers iemand in omdat je ergens zelf geen expertise in hebt. Zou een keurmerk iemand die expertise nodig heeft niet juist kunnen helpen? Het zou ook voor de sector zelf helpen om het kaf van het koren te scheiden. Ik ben oprecht geïnteresseerd in hoe de heer Valize en zijn partij vanuit die twee uitgangspunten aankijken tegen de ontwikkeling of doorontwikkeling van een keurmerk in zijn algemeenheid.

De heer **Valize** (PVV):
Het is lastig om daar een antwoord op te geven, want dat is de portefeuille van mijn collega die daarover gaat. Die heeft de portefeuille Economische Zaken. Daar kan ik dus niet direct een antwoord op geven. Ik weet wel dat wij in ieder geval tegen een ophoging van de regeldruk zijn. Daarom heb ik ook aangegeven: op het moment dat een keurmerk daadwerkelijk iets toevoegt, dan zal het bespreekbaar zijn. Maar op dit moment geldt voor heel veel bedrijven dat zij al met zogenaamde code of conducts werken. Ze hebben een toetsingskader en maken een risico-inventarisatie en -evaluatie. Er wordt gekeken naar de bedrijven waarmee ze zaken doen. Op basis daarvan kan het onderscheid gemaakt worden of een bedrijf een potentieel risico met zich mee kan brengen. Er zijn al heel veel keurmerken die in die richting pleiten. Dat geldt iets minder voor de ontwikkeling van softwarepakketten en digitale hulpmiddelen, maar daarvoor hebben we het CE-keurmerk, dat vanuit de Cyber Resilience Act komt. Alleen, het probleem is dat dat logo bijna identiek is aan het China Export-logo, terwijl daartussenin echt een wereld van verschil zit.

De **voorzitter**:
Ik zie geen verdere vragen van de commissie. Ik geef bij dezen het voorzitterschap weer terug aan u, meneer Valize.

Voorzitter: Valize

De **voorzitter**:
Heel hartelijk dank voor het excellente voorzitterschap. Ik heb begrepen dat ik af en toe een beetje streng kijk, dus ik zal proberen om iets vriendelijker te kijken. Ik kijk even naar mijn rechterzijde. Voor de mensen thuis en op de tribune is dat de linkerzijde. Hoeveel tijd denken jullie ongeveer nodig te hebben? 25 minuutjes? Laten we om 14.15 uur terugkeren naar deze vergadering. Ik schors de vergadering tot 14.15 uur.

De vergadering wordt van 13.43 uur tot 14.15 uur geschorst.

De **voorzitter**:
Een goedemiddag allemaal. Welkom terug bij het commissiedebat Online veiligheid en cybersecurity van de vaste commissie voor Digitale Zaken. Iedereen is weer aanwezig. We zijn aangekomen bij de eerste termijn van de zijde van het kabinet, waarin ik als eerste het woord mag geven aan de heer Van Weel, de minister van Justitie en Veiligheid. Ik stel voor dat wij weer een viertal interrupties toestaan. Ik geef gaarne het woord aan de heer Van Weel.

Minister **Van Weel**:
Dank, voorzitter. Allereerst dank aan de Kamer voor de uitnodiging om met u in debat te

gaan over onlineveiligheid en cybersecurity. Ik zal beginnen met een korte inleidende spreektekst en daarna heb ik een aantal blokjes. Het eerste is de Nederlandse Cybersecuritystrategie, NIS2 en de SER en alle andere afkortingen die zijn langsgekomen. Dan heb ik een kopje weerbaarheid en hybride dreigingen, cybercrime en overige belangrijke onderwerpen.

Laat ik beginnen met mijn inleiding. Dit is een belangrijk onderwerp, want we zien dat in de geopolitiek turbulente tijden statelijke actoren hun activiteiten intensiveren. Ook blijven criminele actoren op grote schaal aanvallen uitvoeren. In andere woorden: de digitale dreiging tegen Nederland is groot en divers. Dat is zorgelijk, want de continuïteit van digitale processen is en blijft essentieel in onze maatschappij. Die zijn onlosmakelijk verbonden met onze nationale veiligheid. Met de implementatie van de Cyberbeveiligingswet verhoogt het kabinet de digitale en de economische weerbaarheid van Nederland. Ruim 8.000 organisaties in Nederland worden verplicht om beveiligingsmaatregelen te nemen. Ook moeten zij voortaan binnen 24 uur melding maken van significante cyberincidenten. De Cyberbeveiligingswet treedt naar verwachting nog voor het einde van het jaar in werking. We roepen organisaties ook op om niet af te wachten, maar om nu al actie te ondernemen om hun digitale processen te beschermen. De risico's die organisaties lopen zijn immers nu al aan de orde van de dag. We lezen daar letterlijk elke dag over in het nieuws omdat het aan de orde van de dag is.

Voorzitter. Voordat ik overga naar het beantwoorden van de vragen, wil ik toch nog één ding memoreren. Vanmorgen was ik met mijn Duitse collega, de minister van Binnenlandse Zaken, Nancy Faeser, in Rotterdam. Wij spraken daar over georganiseerde misdaad, ondermijning en corruptie. Daar trok ik een analogie met de cyberwereld, waarin, als je vijftien jaar terugkijkt, cyber door bedrijven vaak werd gezien als een ondergeschoven kindje. Dat gold ook voor particulieren. Het internet was iets wat de overheid veilig moest houden, en dan zou het allemaal wel goedkomen. Dat werd gevolgd door een periode waarin mensen en bedrijven daadwerkelijk werden aangevallen, maar zij dat graag geheimhielden uit schaamte, zo van: waarom gebeurt dit mij, ik moet hier vooral niets over delen.

Inmiddels staan we aan de vooravond van de invoering van de Cyberbeveiligingswet, die bestuurders van bedrijven gewoon een wettelijke aansprakelijkheid geeft als het gaat om cybersecurity. We zijn in een periode waarin bedrijven snappen dat een CIO gewoon thuishoort aan de boardtafel, dat investeren in cybersecurity ook investeren in de continuïteit van je bedrijf is. Sommigen van u brachten op dat papier geduldig is en dat het gaat om actie. Maar vanmorgen, toen wij het hadden over corruptie, de schaamte en het taboe dat daar nog op ligt, kwam ik erachter dat we eigenlijk in cyber al een heleboel stappen hebben gezet. De evidentie daarvan wat betreft de georganiseerde criminaliteit is overigens ook duidelijk. Het zal je maar gebeuren. De vraag is meer hoe je je ertegen wapent en hoe je ermee omgaat als het je gebeurt. Maar de positieve noot dat we al een heleboel stappen hebben gezet, wil ik wel geven. Echter, het is nooit af. De kloof waar door sommigen van u over werd gesproken, zal altijd blijven bestaan. Bij elk stukje waar wij de kloof dichten, zal er weer getracht worden door criminelen en statelijke actoren om aan de andere kant van de kloof de spelregels weer wat te verzetten. Het is in die zin een ongoing game.

Dat brengt mij bij de vragen van de heer Six Dijkstra over de cyberbasishygiëne. Hoe

zorgen we dat in ieder geval de basis op orde is? Hebben we een inschatting van wat het ons zou schelen? Hoe zetten we het bedrijfsleven aan om hiervoor te zorgen? De constatering in het AP-rapport dat men in twee derde van de onderzochte gevallen de basismaatregelen niet op orde had en dat die gevallen dus vermijdbaar waren, past helemaal binnen het Cybersecuritybeeld Nederland en bij waar de Cyber Security Raad ons ook al voor waarschuwde. Organisaties in Nederland hebben hun basisweerbaarheid nog onvoldoende op orde. Ik deel dus de mening dat naast alle wetgeving de basismaatregelen cruciaal zijn en heel veel leed kunnen voorkomen. Daarom wordt cyberhygiëne — daar vatten we dit onder — verplicht onder de Cyberbeveiligingswet. Het NCSC heeft samen met het Digital Trust Center vijf basismaatregelen voor cyberbeveiliging opgesteld. Die staan op de website. Het NCSC communiceert hier ook regelmatig over. Het is niet mogelijk om een betrouwbare inschatting te maken van de totale omvang van de schade van ransomware, maar er zijn wel verschillende losse onderzoeken. Zo blijkt uit recent wetenschappelijk onderzoek naar ransomware dat bedrijven met herstelbare back-ups 27 keer minder kans hebben om losgeld te betalen. Ik denk dat dit al een incentive op zich zou zijn voor bedrijven om die geringe investering te doen, om zo grotere schade te voorkomen. Ik noem dat hier nogmaals, maar we verwachten daar ook meer in te kunnen doen met de Cyberbeveiligingswet.

Dat hangt samen met uw vraag over de bewustwording in de boardroom. Ik noemde het net al. Vijftien jaar geleden bestond de CIO nog niet. Tien jaar geleden mocht hij bij sommige vergaderingen aanschuiven. Zeven jaar geleden zat hij aan tafel, maar raakte hij altijd zijn budget kwijt als de jaarbegroting rond moest worden gemaakt. Maar inmiddels is echt sprake van een andere situatie. Door de Cyberbeveiligingswet worden bestuurders echt verplicht tot het volgen van trainingen en zijn zij ook aansprakelijk voor het onjuist toepassen van beveiligingsmaatregelen. Ik noemde het al even. Dat zal niet alleen effect hebben op de 8.000 entiteiten die onder de wet komen te vallen. Dankzij afspraken die zij moeten maken met hun toeleveranciers, zal het effect nog veel groter zijn dan dat. In die zin ben ik dus optimistisch over de stappen die wij hebben gemaakt. En er komt nog meer aan.

Er was een vraag van mevrouw Michon-Derkzen over afwegingskaders die kunnen helpen om te bepalen welke sectoren en organisaties andere mogen verdringen bij het ontvangen van prioritaire bijstand, als het zover zou komen. Waaraan moeten cybersecuritybedrijven zich houden als dat zou optreden? Het antwoord is dat voor het Landelijk Crisisplan Digitaal een vertrouwelijke bijlage is opgesteld met daarin een afwegingskader voor vitale processen. Op basis van de geleerde lessen uit ISIDOOR — ik kom daar zo meteen nog even op terug — wordt het afwegingskader verbreed en doorontwikkeld. Ik zei al dat die bijlage vertrouwelijk is. En dat is logisch, want die zou aanvallers inzicht kunnen geven in hoe wij onze afwegingen maken op het moment dat dat echt nodig is. Maar ik kan die bijlage wel vertrouwelijk delen met uw commissie.

U vroeg ook: moet eigenlijk niet het hele land met ISIDOOR oefenen, en hebben bestuurders daarbij dan ook een rol? Hebben de veiligheidsregio's een rol bij de jaarlijkse oefeningen? "Het hele land", weet ik niet. Ik zou dat graag doen, want ik deel met mevrouw Michon-Derkzen dat cybersecurity iets is wat ons allemaal aangaat en dat we daar allemaal bij te leren hebben. Maar de organisatie daarvan wordt dan wel op enig moment wat complex. Maar zowel de bestuurders als de veiligheidsregio's hebben een rol bij de jaarlijkse oefeningen. Aan de ISIDOOR IV-oefening, die we in 2023

hebben gehouden, hebben verschillende veiligheidsregio's meegedaan, waaronder Rotterdam-Rijnmond en Haaglanden, maar ook het cybersecuritysamenwerkingsverband voor de veiligheidsregio's en het LOCC, het Landelijk Operationeel Coördinatie Centrum. Zij oefenen de bestrijding van fysieke gevolgeffecten van een cyberaanval in de samenleving of oefenen bij de jaarlijkse overheidsbrede cyberoefening die is geïnitieerd door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Daarbij ligt de nadruk op de reacties van overheidsorganisaties zelf op een cyberincident, dus: wanneer worden zijzelf getroffen en hoe gaan zij daarvan herstellen?

De veiligheidsregio's zijn absoluut belangrijke partners bij de gezamenlijke aanpak van een cybercrisis, want de gevolgen van een cybercrisis voor de openbare orde en veiligheid worden door die lokale driehoek en door de veiligheidsrisico's bestreden. Daarom is het Landelijk Crisisplan Digitaal ook samen met de veiligheidsregio's opgesteld.

Nu we weten dat we de implementatie van de NIS2-richtlijn niet binnen de gestelde termijn gaan halen, vroeg mevrouw Michon-Derkzen, maar ook mevrouw Koekkoek, wat we doen om entiteiten toch voor te bereiden op de nieuwe wet. Wat kunnen zij de komende tijd verwachten? En zorgen we ervoor dat zij voldoen aan de eisen van de NIS2-richtlijn? Ik zal het u in alle openheid zeggen. Tijdens de informele JBZ-Raad van de afgelopen week in Warschau heb ik meerdere collega's gesproken. Allen bevestigden dat zij bij de zorgvuldige implementatie dezelfde vertraging oplopen als wij of vertelden dat zij de landen die zeiden daarmee wel op tijd te zijn, ervan verdachten niet meer dan een papieren exercitie te hebben gedaan. Daarmee wil ik niks afdoen aan de landen die zeggen dat zij wel op tijd zijn, maar het gaf mij wel inzicht in hoe serieus deze exercitie is en hoeveel daarbij komt kijken. Dit is echt een groot traject. Ik heb dat zelf aan den lijve ondervonden bij een bezoek aan het NCSC. Het is een enorme klus om van een paar honderd klanten in één keer over te gaan naar 8.000 klanten — daar komt het op neer — en die mee te nemen in dezelfde mate van weerbaarheid.

Binnenkort wordt de Cyberbeveiligingswet in uw Kamer behandeld. Het besluit waarin onder andere de zorgplicht wordt uitgewerkt, wordt binnenkort in consultatie gegeven. Onderdeel daarvan is een regeldruktoets. Bij de implementatie wordt zo veel mogelijk aangesloten op de gangbare normen en de cyberbeveiligingspraktijken met als doel om juist bij de entiteiten de lasten te beperken.

De Rijksinspectie Digitale Infrastructuur heeft een NIS2-quickscan ontwikkeld die organisaties adviezen en tips geeft over hoe men zich nu al kan voorbereiden op de NIS2-richtlijn. Daarnaast wordt proactief ingezet op sectoroverstijgende communicatie om elke sector goed te informeren. Ook het NCSC heeft op diens website in meer algemene zin basisprincipes voor digitale hygiëne gepubliceerd.

Van NIS2 ga ik over naar het programma Cyclotron.

De **voorzitter**:
Mevrouw Michon-Derkzen wil u interrumperen.

Mevrouw **Michon-Derkzen** (VVD):
De informatiedichtheid in de antwoorden van deze minister is groot. Houd dat vast. Daar

wil ik dus niks over zeggen, maar misschien ben ik daarom iets te laat. NIS2 zorgt er inderdaad voor dat ook alle toeleveranciers die zorgplicht hebben en bestuurlijk aansprakelijk zijn. Ik hoor de minister zeggen dat dit natuurlijk ook leidt tot iets van een administratieve last, maar ook dat checken we van tevoren, hè? Valt het onderwijs nou ook onder die sector? Eigenlijk willen we het hele ecosysteem via NIS2 — u noemt dat "hygiëne" — op een hoger niveau trekken. Om het goed te begrijpen: als we het hebben over de vitale sector en de toeleveranciers, dan hebben we het ongeveer over heel Nederland, maar zit het onderwijs daar dan wel of niet in?

Minister **Van Weel**:
Het is goed dat mevrouw Michon-Derkzen dat vraagt. Daarover zijn we nog in overleg met het ministerie van Onderwijs, Cultuur en Wetenschap. Op dit moment valt het hoger onderwijs daar niet onder. De Europese richtlijn geeft de ruimte om te bepalen of dat onder de strategische sectoren moet vallen of niet. Een aantal weken geleden hebben we echter gezien dat een grote cyberaanval op een universiteit wel degelijk ook nationale uitstraling heeft. Vanuit die optiek én om ervoor te zorgen dat wij, indien kenniscentra worden aangevallen, er ook met de rest van de entiteiten wat mee kunnen, dat we gewapend zijn tegen wat daar mogelijk gebeurt en dus een goede informatie-uitwisseling hebben, zal mijn pleidooi aan de minister van OCW nogmaals zijn om deze sector wél onder de reikwijdte van de Cyberbeveiligingswet te brengen. Maar daar is nog geen besluit over genomen.

De **voorzitter**:
De minister vervolgt zijn beantwoording.

Minister **Van Weel**:
Dan Cyclotron. Mevrouw Michon-Derkzen vroeg of het programma Cyclotron hét model is om informatie uit te wisselen tussen publieke en private partijen. Het korte antwoord is: ja. Maar om de informatiedichtheid wat groter te maken, voeg ik daar nog het volgende aan toe. Om Nederland een onaantrekkelijk doelwit te maken voor digitale aanvallen, vinden wij het juist belangrijk om publieke en private partijen sneller informatie te laten delen over de dreigingen en incidenten en dat te analyseren. Vandaar dat het programma Cyclotron is gestart om deze samenwerking mogelijk te maken. Het geeft ook invulling aan de behoefte van publieke en private organisaties om intensiever informatie te delen. Dit kabinet heeft de financiering daarvan uit de intensiveringsmiddelen op de begroting van JenV mogelijk gemaakt.

Leert Cyclotron dan ook van de evaluatie van het project Melissa? Zeker, want dat was juist een heel mooi voorbeeld waarbij gezamenlijk werd gewerkt aan de bestrijding van ransomware. We nemen dat dus mee in Cyclotron. Melissa als zodanig komt dus niet terug, maar de lessen daaruit zult u wel terugvinden in Cyclotron. Dat betreft onder andere het scheppen van duidelijke verwachtingen, het stellen van haalbare doelen, het maken van duidelijke werkafspraken en het bouwen aan onderling vertrouwen.

Mevrouw Koekkoek stelde een vraag over de implementatie van alle afkortingen. Ik ga ze hier niet allemaal noemen, al is mijn spreektijd niet beperkt. Hoe verhoudt zich dit tot de digitale weerbaarheid van bedrijven? Moeten we gas bijgeven om het mkb te helpen? Nou, op het mkb zal de minister van Economische Zaken wel terugkomen. De implementatie verloopt verder volgens plan. Ik heb het al gehad over de regelgeving; die proberen we te beperken door aan te sluiten op gangbare cybersecuritynormen. We

doen al het nodige om het bedrijfsleven en in het bijzonder het mkb hierbij te helpen.

De DTC-wet, de subsidies vanuit het DTC en de ondersteuning bij de implementatie van de Cyber Resilience Act zijn allemaal gericht op het mkb. De overige vragen verwijs ik graag door naar de minister van Economische Zaken.

Mevrouw Michon-Derkzen vroeg nog naar de Nederlandse Cybersecuritystrategie. Past die binnen de bestaande strategie of komt er nog een uitbreiding? Het vorige kabinet heeft structureel 111 miljoen euro in cybersecurity geïnvesteerd. Die middelen zijn gekoppeld aan de uitvoering van de Nederlandse Cybersecuritystrategie, die loopt tot 2028. De hoofddoelen daarvan staan dus vast, maar daarbinnen wordt wel elk jaar een actieplan ontwikkeld. Daarover wordt u elk jaar geïnformeerd via het jaarverslag van de begroting van Justitie en Veiligheid. Dat evalueren we elk jaar. Dus als nieuwe zaken nodig zijn, ofwel op basis van de verandering in het dreigingsbeeld ofwel door de eisen die extern aan ons worden gesteld, dan voegen we die erbij. Tegen de heer Valize zeg ik ook dat de inzichten uit het Samenhangend Inspectiebeeld en het Cybersecuritybeeld worden betrokken bij de uitvoering van dit actieplan onder de Nederlandse Cybersecuritystrategie. Overigens hebben de toezichthouders vooruitlopend op de implementatie van de NIS2-richtlijn ook de onderlinge samenwerking geïntensiveerd. Dat waren wat mijn deel betreft de vragen over de verschillende afkortingen, van NLCS tot SIS, CER, DSA et cetera. De minister van Economische Zaken heeft natuurlijk ook nog een aantal zaken.

Dat brengt mij bij het kopje weerbaarheid en hybride dreigingen. Meerderen van u vroegen wat het cyberdeel is van wat er moet gebeuren naar aanleiding van de brief die ik samen met de minister van Defensie begin november aan uw Kamer heb gestuurd over het verhogen van onze weerbaarheid. Nu al is er binnen de uitvoering van de Nederlandse Cybersecuritystrategie op sommige onderwerpen extra inzet geleverd, bijvoorbeeld omdat de veranderende dreiging daarom vroeg. Een voorbeeld daarvan is de verkenning naar actieve cyberbescherming en de extra inzet ten aanzien van een publiek-privaat informatiedelingsplatform, waarover we het net hadden. De cyberstrategie loopt tot 2028. De evaluatie van dit jaar heeft ook als doel om meer inzicht te krijgen in de voortgang en te bezien of in het licht van de weerbaarheidsstrategie eventueel extra inzet nodig is.

Daarnaast is een belangrijke manier om onze weerbaarheidsdoelen uit de brief van november te realiseren het implementeren van een Cyberbeveiligingswet en het realiseren van de Cybersecuritystrategie. Uiteindelijk, als we onze digitale dijken verhogen tegen criminelen, verhogen we ze ook tegen statelijke actoren. In die zin zijn de twee dreigingen niet heel erg onderscheiden van elkaar. Over de strategie in het geheel spreek ik op 10 april nog met uw Kamer. Dat betreft het commissiedebat Nationale veiligheid en weerbaarheid. Maar het allerbelangrijkste — dat raakt ook een van de vragen van u, namelijk op welke begroting dit landt et cetera — is dat wij in het voorjaar terugkomen met een algeheel plan. We zullen dat betrekken bij de besluitvorming over de Voorjaarsnota. In november hebben we geconstateerd wat er ontbreekt en in het voorjaar komen we terug op wat eraan moet worden gedaan, waaraan we prioriteit geven tussen de verschillende sectoren, waar dat landt op de verschillende begrotingen en welke middelen daarvoor nodig zijn. Ik moet heel eerlijk zeggen dat ik niet denk dat cyber ons grootste probleem of onze grootste uitdaging is binnen de brief over weerbaarheid. Nogmaals, ik denk dat we daar juist een heleboel

stappen hebben gezet, terwijl we in andere sectoren zullen zien dat de uitdagingen misschien veel groter zijn. Laat me er eentje noemen als voorbeeld: de weerbaarheid van onze elektriciteitsvoorziening. Waar we jarenlang niet hebben nagedacht over weerbaarheid of de potentie van sabotage of aanvallen, moeten we dat nu wel doen. Dat zijn natuurlijk hele grote uitdagingen.

Mevrouw Michon-Derkzen vroeg wat we doen in een situatie waarin alles uitvalt: de bank, publieke diensten, stoplichten, mobiele telefoons. Hoe pakken we dan de rapid response aan? Ik zou u willen wijzen op een televisie-uitzending van twee maanden geleden waaraan ik heb deelgenomen. Die uitzending heette Black-out en was van de EO. Daarin werd juist dit scenario behandeld. Hoe ga je nou om met een situatie waarin je twee weken zonder stroom zit, zonder voorzieningen zit? Wat doet dat met een maatschappij? Ik denk dat de allereerste les eigenlijk is — die geldt voor iedereen in dit land — dat je moet zorgen dat je iets van zelfvoorzienendheid hebt. Ik weet dat er vaak lacherig wordt gedaan over noodpakketten en of je die in huis moet hebben, met daarin batterijen, kaarsen, zaklampen, voedsel et cetera, maar daar komt het uiteindelijk wel op neer. Zeker als er in onze digitaal verweven maatschappij sprake is van grote crises of grootschalige uitval, zal een overheid ook in het begin bezig zijn om de meest kritieke diensten die van landsbelang zijn weer up and running te krijgen. U kunt zich voorstellen dat stoplichten daar dan even niet bij zitten en wellicht ook de lokale elektriciteits- of energievoorziening niet. Het hebben van een zekere mate van resilience is dus aan te bevelen.

Op dat punt nog iets anekdotisch. Ik vertelde aan …

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

De heer **Six Dijkstra** (NSC):
Ik was net benieuwd naar de anekdote, maar ik zal mijn vraag eerst stellen.

Ik ben best een groot voorstander van dit soort programma's als het gaat om bewustwording en weerbaarheid en van het programma Black-out met de minister, maar in het verleden ook ISIDOOR. Ik sla eigenlijk ook wel aan op wat collega Michon-Derkzen zei over het betrekken van burgers bij dit soort oefeningen. Ik snap dat we niet alle 18 miljoen mensen in Nederland kunnen betrekken bij een grootschalige oefening, maar het is natuurlijk wel nuttige informatie om te kijken hoe een gemiddelde burger zal reageren op een crisissituatie, dus niet alleen de bestuurders, degenen met eindverantwoordelijkheid, maar ook de mensen die opeens te kampen hebben met uitvallende elektriciteit of een mobiele storing of andersoortige voorstelbare dreigingen waar we de komende tijd mee te maken hebben. In welke mate betrekt de minister dat ook bij alle oefeningen en initiatieven die gaande zijn of die er nog aan gaan komen?

Minister **Van Weel**:
Ik neem dat zeker mee in de uitwerking van de Kamerbrief. Een van de concrete voorstellen waar mijn Zweedse collega voor weerbaarheid op dit moment aan werkt, is burgers in staat stellen om cursussen te volgen op diverse terreinen waarvan je denkt dat ze van nut zouden kunnen zijn in tijden van crisis. Denk bijvoorbeeld aan het kunnen repareren van basiselektriciteitsvoorzieningen. Daar zou je natuurlijk ook cyberweerbaarheid aan kunnen koppelen. Hij had het zelf over EHBO-trainingen. You

name it. Je kunt je dus voorstellen dat je mensen aanbiedt om een extra skill te leren die ze periodiek kunnen bijhouden en waarmee ze in het geval van een crisis, omdat mensen nu eenmaal verspreid zijn over het hele land, daadwerkelijk lokaal de maatschappij draaiende kunnen houden. Ik vind dat heel interessante gedachtes en die wil ik hierin zeker meenemen. Daar hoort cyber wat mij betreft bij.

Dan toch de anekdote, om u niet in al te veel spanning naar huis te laten gaan. Die was van een andere noordse collega, tegen wie ik vertelde dat wij in deze brief hadden aangekondigd dat wij aan de Nederlandse bevolking vroegen om ook 48 uur zelfredzaam te zijn. Toen viel hij van zijn stoel en zei: "48 uur? Dat kun je naakt ondersteboven hangend aan een boom in de sneeuw nog wel volhouden." Om maar aan te geven: zij waren inmiddels aan het oprekken naar een week en het buurland naar twee weken, dus we hebben nog wel wat te doen.

Maar wat doen we dan vanuit het NCSC op het moment dat zich zo'n crisis voordoet? Het NCSC is verantwoordelijk voor incidentrespons op het moment dat dit soort vitale organisaties wordt geraakt. Die organisaties kunnen zelf dan ook melding doen bij het NCSC. De bijstand kan bijvoorbeeld bestaan uit advies over de afhandeling van ICT-incidenten, het ter plaatse gaan en hulp leveren, of het opstellen van een situationeel beeld. Het NCSC werkt daarbij ook samen met andere partijen. Zo zijn er meerdere sectorale CERT's waar organisaties terechtkunnen voor bijstand bij cyberincidenten, zoals het Z-CERT voor de Nederlandse zorg.

Dan nog in aanvulling op het continuïteitplan, dus herstelplannen in de vitale sectoren. Mevrouw Kathmann vroeg daarnaar. De Cyberbeveiligingswet treedt naar verwachting in het derde kwartaal van dit jaar in werking. Alle 8.000 organisaties die daaronder komen te vallen, worden verplicht tot het nemen van beveiligingsmaatregelen. Wat die precies inhouden, komt te staan in het Cyberbeveiligingsbesluit, dat in consultatie gaat, zoals ik eerder zei. Maar onderdeel daarvan is dat die entiteiten ook continuïteit- en herstelplannen hebben. Het uitgangspunt is ook daar om niet strikt vast te houden aan die 48 uur, omdat dit per sector en per incident kan verschillen. Ik denk dat ik voor wat betreft weerbaarheid alle onderwerpen wel heb behandeld.

Ik kom bij het kopje cybercrime. Er was eigenlijk maar één specifieke vraag. Die was van de heer Six Dijkstra over de darkwebplatformen en de populariteit daarvan: hoe kijken wij aan tegen het actief vervolgen van kleine aanbieders van gestolen data? De toestroom van vaak jonge low-levelcybercriminelen, die vooral erkenning willen en willen experimenteren, is een bekend en zorgwekkend probleem. De politie doet samen met de Haagse Hogeschool onderzoek om meer te leren over de ontwikkeling van criminelen en om hier ook effectiever op de goede momenten in te kunnen interveniëren. Zo ontwikkelt de politie methoden en interventies om cybercrime breed te bestrijden. Er wordt niet alleen gekeken naar het aanhouden van verdachten, maar ook naar de mogelijkheden voor preventie en verstoring, waaronder het voorkomen en verstoren van daderschap op dit soort platforms. In de Kamerbrief over de integrale aanpak van cybercrime van juni jongstleden werd uitgebreider ingegaan op de aanpak en het cybercrimebeeld van de politie hierbij. De onlinecriminaliteit komen we natuurlijk ook tegen in andere debatten.

Dan heb ik nog een aantal overige belangrijke vragen. Een daarvan ging over "Q-Day", zoals ik het maar even noem. Dat is dan niet Queen's Day, zoals we die ooit kenden,

maar de dag dat de kwantumcomputer ons leven komt verrijken; in sommige opzichten kan die het ook verpesten. Zowel de heer Six Dijkstra als mevrouw Koekkoek van Volt vroegen daarnaar. We waarschuwen daar als kabinet al enige tijd voor, zeker voor het "store now, decrypt later"-scenario. Het Post-quantumcryptografiemigratiehandboek van TNO, CWI en AIVD waarschuwt hier ook voor en biedt handelingsperspectief aan actoren voor dit scenario. Het scenario is ook opgenomen in het Cybersecuritybeeld Nederland 2024. Ik zeg het hier nogmaals voor iedereen die luistert: ik vind het belangrijk dat organisaties in Nederland dit risico opnemen in hun eigen risicomanagementbeleid en dat ze ook passende maatregelen treffen om het risico en de impact te minimaliseren. Nogmaals, ik verwijs naar het handboek, want dat geeft organisaties vrij eenvoudige mogelijkheden om zich tegen dit scenario te wapenen.

Ik had nog een vraag van mevrouw Michon-Derkzen over keurmerken in aanbestedingen van de overheid.

De **voorzitter**:
U heeft een interruptie van mevrouw Koekkoek van Volt.

Mevrouw **Koekkoek** (Volt):
De minister gaf terecht aan dat we dat handboek met handelingsperspectief hebben. Ik maak mij er zelf nog wel zorgen over dat er best veel gevraagd wordt van bedrijven. We kijken nu ook naar kortetermijncyber, maar ik kan me voorstellen dat je op een gegeven moment door de bomen het bos niet meer ziet. In die context zou ik willen vragen of zo'n handboek voldoende is en hoe we dat een beetje bijhouden. Als je de zaken rondom de kwantumdreiging voor bedrijven niet goed op orde hebt, wordt een behoorlijk deel van de samenleving kwetsbaar. Dat zagen we bij cyber en mijn zorg is dat je dit straks bij kwantum ook gaat zien. Is daar ook enige sturing voor nodig?

Minister **Van Weel**:
Ik ga daar serieus naar kijken, zeg ik tegen mevrouw Koekkoek. Ik verwacht niet dat de kwantumdreiging voor alle bedrijven de grootste dreiging is die op ze afkomt. Heel vaak gaat het over gevoelige informatie, zeker wanneer we het hebben over store now, decrypt later. Denk aan het recept van Coca-Cola of aan de vraag hoe je een euv-machine van ASML in elkaar zet. Dat soort bedrijven moeten er serieus rekening mee houden dat de encryptie die ze gebruiken over een tijdje ervoor kan zorgen dat dit soort informatie toch toegankelijk wordt. Dat is natuurlijk niet voor alle bedrijven het grootste risico, maar we gaan ook te maken krijgen met kwantumcomputers die aanvallen kunnen uitvoeren op complexe netwerken. Dat wordt natuurlijk wel een probleem waar iedereen mee te maken krijgt, al denk ik niet dat dit meteen op dag één gebeurt. Maar ik vind het een interessante gedachte om te kijken hoe we dat meer toegankelijk kunnen maken, ook voor de brede gemeenschap.

De **voorzitter**:
Dan heeft u nog een vervolgvraag van mevrouw Koekkoek.

Mevrouw **Koekkoek** (Volt):
Ik maak me vooral zorgen over het tweede dat de minister aanstipt. Kijk, grotere bedrijven die toch al een bepaald systeem dragen, zullen zich er ook eerder van bewust zijn en zullen ook de middelen hebben om een systeemrisico aan te pakken. Maar van het tweede punt dat de minister zelf noemde, vraag ik me af of we dat nu al wat

concreter zouden kunnen maken. Ik vind het goed dat ernaar gekeken wordt, maar is er ook een manier om dat bij te houden zonder dat je meteen weer alle lasten bij bedrijven zelf legt? Zou je daar misschien sturing op kunnen geven middels bijvoorbeeld een realistisch tijdpad, zo van: over zoveel jaar zou het belangrijk zijn als u als bedrijf dit en dit gedaan heeft? Als we daar wat richting in geven, kan een bedrijf zelf ook toetsen of het op de goede weg is.

Minister **Van Weel**:
Ik laat deze vraag deels aan de minister van Economische Zaken. Ik denk dat hij er ook wel ideeën bij heeft, gewoon vanuit hoe je bedrijven klaarmaakt voor the quantum age, om het zo maar te zeggen. Vanuit de dreigingskant zijn er een aantal dingen die we kunnen voorspellen en een aantal dingen die we nog helemaal niet kunnen voorspellen hier. We moeten dat bijhouden en we moeten erover communiceren, maar ik vind het moeilijk te duiden wat het betekent voor individuele actoren. Maar nogmaals, de toezegging heeft u dat we gaan kijken hoe we dit toegankelijk kunnen maken.

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

De heer **Six Dijkstra** (NSC):
Mijn vraag aan de minister over Q-Day ging niet zozeer om het handelingsperspectief voor bedrijven, maar meer om individuele burgers. Het is gewoon een heel reëel scenario dat veel van hun privégegevens die ze nu versturen en nu bewaren op een gegeven moment openbaar zullen worden gemaakt omdat die nu ergens door een Chinese of een Russische actor opgeslagen worden en later ontsleuteld worden. Dat kan in het ergste geval best wel voor maatschappelijke onrust of zelfs paniek zorgen. Dat kan een ontwrichtend effect hebben. Mijn vraag aan de minister was ook of het kabinet impactscenario's heeft uitgewerkt, afhankelijk van hoe Q-Day eruit zal zien, ook om ervoor te zorgen dat mensen erop voorbereid zijn dat dit een reëel scenario is in de toekomst.

Minister **Van Weel**:
Nee, dat denk ik niet, op dit moment. Ik zeg niet dat dit scenario niet denkbaar is, want dat zou kunnen. Mijn eerste zorg op dit moment zou zijn het gemak waarmee mensen hun eigen gegevens zelf al weggeven aan bedrijven, al dan niet in China gevestigd, zonder dat daar kwantumdecryptie aan ten grondslag ligt. Ik zit ook op een paar socialmediasites — ik zal niet zeggen welke — maar ik schrik zelf ook weleens van de ads die ik voorgeschoteld krijg op basis van iets waar ik naar mijn eigen idee alleen nog maar aan gedacht had en van wat daar aan data harvesting achter zit. Ik zou toch willen meegeven aan iedereen hier dat als je ergens niet voor betaalt of hoeft te betalen, je met jezelf betaalt, namelijk met de data die je zelf achterlaat. Dat zou mijn zorg zijn nu. Die data kunnen op een gegeven moment ook tegen ons gebruikt worden. Dat is meer in algemene zin. En natuurlijk: met het breken van encryptie wordt dat probleem groter, maar blijft dat probleem wel hetzelfde.

De **voorzitter**:
Dan heeft u daar nog een vervolgvraag op van de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Uiteraard deel ik die zorg van de minister, maar er zijn natuurlijk best wel veel

chat-/communicatieapps, zoals WhatsApp en Signal, die de belofte van end-to-endencryptie doen, waarbij de data die je verstuurt naar iemand alleen tussen jou en hem blijft. Heel veel mensen appen met hun geliefde en hun dierbaren en sturen gegevens over de lijn die ze graag liever niet online willen zetten, waar ze ook heel bewust over nadenken. Maar met de kwantumcomputer is het risico dat dit over een aantal jaar, als dat geharvest is door statelijke actoren, wel tegen hen gebruikt kan worden. Dat terwijl ze ervan uitgaan dat het in vertrouwelijkheid is. Dat vind ik wel een reëel risico, dat over een aantal jaar echt een flink grote maatschappelijke impact kan hebben. Hoe kijkt de minister daartegen aan?

Minister **Van Weel**:
Ik zou zeggen: dat risico bestaat ook nu. De chatdiensten die we nu hebben, zijn niet onbreekbaar. Zo dachten grote criminele netwerken ook dat ze met EncroChat en Skynet onzichtbaar waren voor in dit geval justitie. Ook daar zie je dat uiteindelijk de codes van die netwerken gebroken worden. In dit geval is dat gebeurd door onze eigen opsporingsdiensten, die die informatie hebben gebruikt om strafbare feiten te kunnen opsporen en netwerken te kunnen blootleggen. Maar je kunt ook nu al niet uitsluiten dat statelijke actoren die interesse hebben in bijvoorbeeld mijn handel en wandel, dat proberen ook via WhatsApp te doen. Dat is echt niet in alle gevallen interessant. Zeker bij mij, zou ik nu via u tot de Chinezen willen zeggen: doe het niet. Maar het is een risico en daar moeten we burgers op voorbereiden. Dat doen we. We komen periodiek met dreigingsbeelden vanuit het NCSC en dat zullen we blijven doen. Dat zullen we ook doen over kwantumdreiging.

De **voorzitter**:
Dus preventief geen pikante foto's over en weer. Vervolgt u uw beantwoording.

Minister **Van Weel**:
Dat is uw invulling, voorzitter.

Ik heb nog één vraag van mevrouw Michon-Derkzen, die gaat over de keurmerken in aanbestedingen van de overheid: kunnen we daarnaar uitvragen? We kunnen niet in een aanbesteding alleen een specifiek keurmerk voorschrijven. De inschrijvende partij moet altijd de gelegenheid krijgen om aan te tonen dat de onderliggende eisen uit het keurmerk kunnen worden gehaald. Bij de overheid worden aanbestedingen gedaan op basis van een risicoanalyse. Op basis daarvan worden gezamenlijk relevante inkoopeisen bepaald en meegenomen in de aanbesteding. De mate waarin certificeringseisen en keurmerken worden meegestuurd in aanbestedingen, is afhankelijk van het resultaat van de risicoanalyse. Ik geloof dat de minister van Economische Zaken nog kort zal ingaan op het bestaan van keurmerken in de sector in algemene zin en op wat dat zou kunnen betekenen voor bedrijven.

Dat was de beantwoording van de aan mij gestelde vragen, voorzitter.

De **voorzitter**:
Heel hartelijk dank, minister Van Weel. U heeft nog een interruptie van mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik heb nog één vraag, waarvan ik denk dat die wel bij minister Van Weel thuishoort. Ik

stelde een vraag over de actie die de politie met heel groot succes heeft uitgevoerd rondom de feestdagen en Black Friday, tegenwoordig Black Friday Week en Weekend. Die actie was gewoon een heel groot succes, niet alleen de actie zelf, maar ook campagnematig. Deze heeft heel veel bereik gehad. We hebben eigenlijk heel snel en heel hard zulk soort acties nodig — meer van dat, opgeschaald. Hoe gaat de minister ervoor zorgen dat dit mogelijk wordt gemaakt?

De **voorzitter**:
De minister. Zeven dagen vrijdag.

Minister **Van Weel**:
Dank dat mevrouw Kathmann mij aan deze vraag herinnert. Inderdaad was dit een uiterst succesvolle actie. Het is overigens schrikbarend als je ziet hoeveel mensen uiteindelijk toch in deze val trapten — want dat was het — waarbij het oude Engelse gezegde "if something looks too good to be true, then probably it is" altijd weer opgeld doet, ook hier dus. Daar gaan we mee door, want dit is een hele confronterende manier voor mensen om erachter te komen: o ja, inderdaad; zo makkelijk trap je dus ergens in. Dat zou je niet doen op de hoek van de straat met die verkoper die je een Rolex probeert aan te smeren. Daarvan weten we dat dat niet klopt. Maar online hebben we die terughoudendheid op de een of andere manier minder. Die moeten we trainen, en daar horen dit soort acties bij. We hebben flink wat extra geld uit de intensivering uitgetrokken voor het bestrijden van onlinecriminaliteit en -fraude. Dat zal ook hieraan worden besteed.

De **voorzitter**:
Dan dank ik u heel hartelijk voor de beantwoording. Dan gaan we door naar de … O, u heeft toch nog een interruptie van mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ja, want die is tweeledig. Ik had ook een vraag gesteld over de cyberweerbaarheidskloof. Eigenlijk zei de minister zelf: als je betaalde apps niet betaalt of misschien niet kán betalen — dat is ook onderdeel van de cyberweerbaarheidskloof — dan betaal je met je data. In the end kunnen die data tegen ons allemaal gebruikt worden. Wat is dan de inzet? Wat doen we eraan, heel concreet, om die cyberweerbaarheidskloof te dichten? We moeten echt hierop gaan inzetten, want cybercriminelen zijn op zoek naar de zwakste schakel, zowel bij bedrijven als bij particulieren. Er wordt wel wat over gezegd en het wordt aangeraakt in de stukken die ik van het kabinet krijg, maar heel concreet wordt het niet. Dus wat zijn nou echt de concrete doelen die worden gesteld en wat gaan we doen om die doelen te halen? Ik denk dat die vraag voor een deel, voor de bedrijven, bij de minister van Economische Zaken ligt, maar waarschijnlijk ook voor een deel bij u omdat het ook gaat over particulieren.

Minister **Van Weel**:
Zoals ik zei, is het een kat-en-muisspel. Zoals criminelen in de echte wereld altijd zullen proberen om op een illegale manier aan geld of aan hun gerief te komen, en daarvoor de makkelijkste methode kiezen, zo doen criminelen dat ook online. Dat gaat nooit meer weg. In die zin moet je dus zorgen dat je je hele maatschappij naar een hoger plan trekt als het gaat om weerbaarheid. Dat begint echt met de basics. De meeste mensen klikken zelf op een link. De meeste mensen hebben 1234 of 0000 als pincode. De

meeste mensen hebben hetzelfde password, en dan van 1 tot 99. We moeten dus allemaal beseffen dat wij hier allemaal kwetsbaar voor zijn en dat we allemaal een verantwoordelijkheid hebben om daar wat mee te doen. Daar kunnen wij wat qua voorlichting voor doen; daar doet het NCSC veel in voor bedrijven. Dat is de basis. Ik denk dat het dichten van die kloof er elke keer uit bestaat om snel nieuwe methoden van criminelen te onderkennen en die meteen door te sluizen en breed bekend te stellen bij bedrijven en de bevolking, om zo iedereen in staat te stellen die eigen weerbaarheid op orde te krijgen.

De **voorzitter**:
Dan is er nog een vervolgvraag van mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Een concreet voorstel dat ik net noemde, dat ik al eerder heb gedaan en waar GroenLinks-PvdA al eerder voor heeft gepleit, is om te komen met een lijst van betrouwbare, gratis opensourcecybersecuritysoftware. Hiermee worden mensen er niet alleen op geattendeerd dat ze een goed password moeten hebben en dat ze dit en dat moeten doen, maar ook op: u vindt die software hier, en hier heb je een goede wachtwoordmanager. Als we daar nou eens een mooie lijst van publiceren, zorgen we in ieder geval dat mensen met weinig knaken — dat is ook een grote oorzaak van die kloof — in ieder geval weten hoe ze met weinig geld, of misschien zelfs wel gratis, toch hun veiligheid op orde kunnen krijgen.

Minister **Van Weel**:
Ik wil er wel naar kijken. We kunnen dat in een volgende halfjaarupdate meenemen. Overigens ben ik van mening dat geld hier in een heleboel gevallen niet het probleem is. Het is niet zo dat mensen cyberveiligheid niet kunnen betalen; het probleem is dat mensen domme dingen doen online. Of ze geld hebben of niet, heeft er vaak heel weinig mee te maken. Het creëren van awareness en het zorgen dat mensen elke keer een update op hun telefoon installeren op het moment dat die binnenkomt, zijn de dingen die echt het verschil maken om die kloof te dichten.

De **voorzitter**:
De minister nodigt u uit, dus moet ik dat zien als een verhelderende vraag?

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dat klopt, want ik voel me heel erg uitgedaagd. Ik ben het ermee eens dat de grootste oorzaak vaak is … Maar dat komt ook omdat een foutje maken menselijk is en we toch weer de makkelijke weg willen kiezen, en noem maar op. Maar ik wil toch wel kwijt dat geld hier een heel groot probleem is. De minister zei het zelf eigenlijk ook al. Als je bijvoorbeeld bepaalde apps niet betaalt, word je gek gemaakt met reclames en spam en kom je veel makkelijker in een onveilige wereld. Ook alleen al in de vorm van wat je voorgeschoteld krijgt. Dat krijg je niet voorgeschoteld als je gewoon geld hebt om alles fatsoenlijk te betalen. En zo is het ook vaak met de smartphones: de duurste hebben de beste beveiliging. Je moet tegenwoordig ook extra betalen bij providers als je veilig wil zijn. Heel veel mensen doen dat niet omdat hun internetabonnement al zo duur is. Ik wil hier dus toch wel even een pleidooi houden dat het zeker ook met de dikte van de portemonnee te maken kan hebben hoe cyberveilig iemand is.

Minister **Van Weel**:

Ja, jeetje, er wordt nu een heel groot thema gehangen aan cyberveiligheid, alsof dat een kloof zou zijn tussen arm en rijk. Ik bestrijd dat. Ik denk niet dat dat zo is. Ik denk dat gedrag en, zoals ik eerder zei, onwetendheid eigenlijk de grootste factoren zijn voor de kloof. Ik geloof dus niet dat het al dan niet betalen voor apps of het niet weten waar je gratis cybersecuritysoftware kunt vinden het grootste probleem is waar we hiermee te maken hebben. Maar nogmaals, dat is mijn inschatting. Overigens bestaat er wel de website veiliginternet.nl. Dat is een heel overzicht van ten eerste de dingen die je beter niet kunt doen dan wel, en ten tweede gratis software waarmee je je beveiliging beter kunt maken. Er zijn natuurlijk ook gewoon Europese richtlijnen die eisen stellen, ook aan dit soort bedrijven, aan wat voor reclame ze mogen hebben en wat niet misleidend mag zijn et cetera. Ik zie het probleem dus veel meer daarin. Ik zou ook niet weten wat dan de oplossing is als geld het probleem is, en alleen geld, zoals u het schetst. Moeten we hier dan geld voor geven? Ik ben hier niet om vragen te stellen aan mevrouw Kathmann, maar ik zie dat niet als oplossing. Ik zie de oplossing echt in: hoe leren we mensen beter gebruik te maken van de middelen die er zijn?

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik wil hier geen gek debat van maken, want volgens mij heb ik helemaal niet gezegd dat geld de enige reden is waarom we in een cyberweerbaarheidskloof kunnen zitten. Volgens mij heb ik het woord "kan" gebruikt. Het heeft er af en toe mee te maken en ik heb daar concrete voorbeelden van genoemd. De minister zei net dat hij met zijn Duitse collega op werkbezoek is geweest in Rotterdam. Ik neem u graag mee naar mijn eigen wijk Spangen, waar heel veel mensen tegen deze problemen aanlopen, omdat hun provider, zoals ik net al zei, hun vraagt om extra te betalen, bijvoorbeeld om veiliger te zijn in het gewone huis-tuin-en-keukengebruik van internet. De duurste smartphones zijn de veiligste smartphones. Je kan veel meer spam verwachten als je niet betaalt voor apps dan wanneer je dat wel doet, omdat je dan op gekke reclames gaat klikken. Ik zeg dus helemaal niet dat geld hét probleem is en dat we dit probleem daardoor hebben. Gedrag is een héél groot probleem, maar ik wil hier wel adresseren dat geld zeker óók een probleem kan zijn. Daarom vroeg ik concreet welke plannen er zijn om die kloof te dichten. Daar hoort ook een plan bij, misschien voor mensen voor wie geld het probleem is in plaats van gedrag, want er zijn ook providers die geen geld vragen voor extra beveiliging op je internetpakket. Laat dat dan bijvoorbeeld de norm zijn in Nederland; daar heb je 'm al. Dat scheelt toch weer een volle boodschappentas per jaar.

De **voorzitter**:
U heeft uw punt heel helder gemaakt. Wil de minister daar nog op reageren? Nee. Dan geef ik het woord aan de volgende spreker van de zijde van het kabinet. Dat is de heer Beljaarts, minister van Economische Zaken.

Minister **Beljaarts**:
Dank, voorzitter. Dank aan de leden voor de vragen. Het behoeft geen toelichting dat digitalisering een drijvende kracht is voor onze economie. Sterker nog, zij vormt ook de ruggengraat van de economische groei en de innovatie in de komende decennia. Een essentiële randvoorwaarde hierbij is dat we als samenleving digitaal veilig en weerbaar zijn. We moeten dus zorgen dat onze cybersecurity op orde is. Nog altijd zijn veel ondernemers slachtoffer van cyberincidenten en worden basismaatregelen onvoldoende doorgevoerd; we hebben meerdere voorbeelden voorbij zien komen. Zo blijkt ook uit onderzoek dat een derde van de kleine bedrijven geen actie onderneemt om online veilig te zijn, terwijl het aantal cyberaanvallen op ondernemers juist toeneemt. Het is dus

meer dan ooit van belang dat ondernemers werk maken van hun digitale weerbaarheid. Het Digital Trust Center is hierbij hét loket van de overheid dat hen helpen kan. Het Digital Trust Center biedt laagdrempelige informatie, advies en tools voor maatregelen die ondernemers kunnen nemen. Ook is er een jaarlijkse subsidie beschikbaar voor ondernemers om de cyberweerbaarheid te verhogen via de regeling Mijn Cyberweerbare Zaak. Zzp'ers en kleine ondernemers kunnen subsidie krijgen voor de kosten van de aanschaf en de implementatie van belangrijke basismaatregelen, zoals back-ups, inloggen met meer factoren of een wachtwoordenkluis.

Op de website van het DTC staan verhalen van ondernemers die dit hebben gedaan en hoe het hen heeft geholpen, peer-to-peer en recommandatie. Daarnaast waarschuwt het DTC ondernemers gevraagd en ongevraagd voor actuele digitale dreigingen en risico's en is er een onlinecommunity waarin 5.700 ondernemers elkaar verder helpen.

In de agenda voor cybersecuritytechnologieën onder de Nationale Technologiestrategie is de ambitie opgenomen om de concurrentie- en kennispositie rondom cybersecurity van Nederland te verbeteren. Daarom zetten we ook proactief in op het intensiveren van de publiek-private samenwerkingen.

Voorzitter. Misschien toch een cri de coeur, want we doen vanuit overheidswege natuurlijk heel veel aan het informeren en voorkomen van cyberdreigingen, maar bedrijven doen er van groot tot klein natuurlijk altijd verstandig aan om ook zelf hun verantwoordelijkheid te nemen en deze verantwoordelijkheid in de toekomst ook te intensiveren.

Voorzitter. Ik heb de beantwoording in vier blokjes ingedeeld: als eerste het Digital Trust Center en mkb, als tweede keurmerken, als derde innovatie, onderwijs en cybersecurity en als vierde overig.

Ik begin graag met een gecombineerde vraag van mevrouw Michon-Derkzen en de heer Valize over het Digital Trust Center en het Nationaal Cyber Security Centrum: is dat een goed toegankelijk aanspreekpunt en heb ik daarmee contact gehad met het mkb? Het nieuwe Nationaal Cyber Security Centrum is er straks voor alle organisaties in Nederland, dus ook voor alle mkb'ers. Hier wordt de dienstverlening van het vernieuwde Nationaal Cyber Security Centrum ook op aangepast. Het uitgangspunt is dat het beste van beide organisaties wordt gecombineerd. Er wordt zorgvuldig gekeken naar de dienstverlening die op dit moment door beide partijen wordt aangeboden en hoe die straks in het vernieuwde centrum een plek kan krijgen. Daarbij is er ook oog voor de verschillen in de behoeften van de verschillende doelgroepen, en er wordt gekeken naar de verschillende producten en diensten waarmee de doelgroepen op een passende wijze kunnen worden bereikt. Het mkb is daarbinnen natuurlijk een hele belangrijke doelgroep. Hierover hebben we natuurlijk ook contact gehad met MKB-Nederland en VNO-NCW.

Mevrouw Michon-Derkzen vroeg ook naar de kloof tussen cyberveiligheid en hoe kleine bedrijven daarmee omgaan. Dat is een terechte vraag; dank daarvoor. Het Digital Trust Center voorziet niet-vitale bedrijven, waaronder juist het mkb, van informatie, maar ook van de tools en de subsidies waar ik net aan refereerde. Daarnaast zijn het Nationaal Cyber Security Centrum en het Digital Trust Center samen op basis van de toekomstvisie met de cyberweerbaarheidsnetwerken aan de slag gegaan met het

bouwplan, dat de praktische inrichting wordt van het Cyberweerbaarheidsnetwerk. Ook daarin wordt expliciet gekeken naar het mkb. Zo wordt het mkb direct of via aangewezen schakelorganisaties geïnformeerd. Die schakelorganisaties kunnen bijvoorbeeld brancheorganisaties, banken, boekhouders of accountants zijn die hun achterban goed kennen en die op die manier ook zzp'ers en kleine organisaties bijstaan. Die schakelorganisaties kunnen dan ook een extra bijdrage leveren aan de cyberweerbaarheid van hun klanten en daarmee het gat dichten in die cyberweerbaarheidskloof.

Mevrouw Kathmann vroeg mij wat ik vind van gratis opensourcetools die aangeboden worden.

De **voorzitter**:
Excuus, u heeft nog een interruptie van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Sorry, het gaat over het DTC en het NCSC; want anders gaan we naar een ander onderwerp. Wanneer is die fusie tot eigenlijk een nieuwe organisatie gereed? Iedereen die weleens in een organisatie heeft gewerkt, weet dat een organisatie die in transitie is, vooral druk is met zichzelf. Dus hoe weten we en hoe toetst de minister dat de mkb-bedrijven die dit zo nodig hebben, de dienstverlening ook tijdens deze verbouwing blijven weten te vinden?

Minister **Beljaarts**:
Dank voor de vraag, want dat is een terechte constatering. Vaak is dat zo. Ik heb geen vooruitziende blik op het komende jaar. Dit moet immers op 1 januari 2026 een feit zijn. Beide organisaties hebben nu een hele belangrijke rol. De integratie moet zorgen dat de dienstverlening breder en beter wordt en dat de dienstverlening along the way verslechtert. Dat is dus absoluut de intentie. Vanuit EZ blijven we opdrachtgever en ook betrokken bij de nieuwe organisatie, juist om te borgen dat ook die dienstverlening aan het bedrijfsleven en het mkb geborgd is. Ik heb dus geen enkele aanleiding om ervan uit te gaan dat de dienstverlening in dit lopende jaar zal verslechteren vanwege het feit dat men bezig is met die fusie.

De **voorzitter**:
Dan mag u verder met uw bijdrage.

Minister **Beljaarts**:
Mevrouw Kathmann had een vraag gesteld over de opensourcetools. Het is uiteraard goed dat die opensourcetools beschikbaar zijn. Die kunnen natuurlijk altijd helpen om de cybersecurity te verbeteren. Daarbij wil ik wel de kanttekening maken dat opensourcecybersecuritysoftware technisch moeilijk te gebruiken is voor de gemiddelde Nederlander of het gemiddelde bedrijf. Het is dus iets meer voor technische specialisten.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Het voorstel is gewoon concreet: kan er gewoon een lijst gepubliceerd worden met betrouwbare gratis opensourcecybersecuritysoftware die gebruikt kan worden? Ik had zojuist al een debatje met de minister van JenV over particulieren, maar dit geldt juist ook voor bedrijven, want heel veel mkb'ers geven aan dat het heel fijn is dat er een hele cybersecuritymarkt is ontstaan, omdat we daardoor heel veel dingen hebben die het

veilig kunnen maken, maar dat de prijs hierdoor ook flink wordt opgedreven. Als je als mkb'er veilig wil zijn, heb je dus diepe zakken nodig. Die zijn er niet altijd. Dus als er centraal in ieder geval zo'n lijst van opensourcesoftware kan komen die gratis is — daar zitten ook echt dingen bij die technisch wat minder moeilijk zijn — scheelt dat in ieder geval altijd in het geld.

De **voorzitter**:
Het woord is aan de minister. Ik wil wel opgemerkt hebben dat dit de vierde interruptie was van mevrouw Kathmann, dus eigenlijk ook de laatste. Een punt van orde?

Mevrouw **Kathmann** (GroenLinks-PvdA):
Daar waren ook een aantal verduidelijkende vragen bij. Er werd mij ook een vraag gesteld door de minister zelf. Ik neem aan dat mijn antwoord daarop niet als een interruptie wordt geteld.

De **voorzitter**:
Die hebben we inderdaad niet meegeteld. Continueert u uw bijdrage, minister.

Minister **Beljaarts**:
Dank, voorzitter. Veiliginternetten.nl is beschikbaar voor iedereen, zowel voor ondernemers als voor consumenten; daar refereerde de minister van Justitie en Veiligheid zojuist al aan. Maar misschien ook daarbij een kanttekening: als er iemand empathie heeft voor mkb'ers die in een financieel moeilijke situatie zitten, dan is dat ondergetekende, maar er is ook zoiets als met een goed verstand weten wat je weggeeft als je op verdachte links klikt en dat soort zaken. Dat is een eigen verantwoordelijkheid die elke ondernemer en burger heeft, los van de portemonnee. In de businessvoering is het uiteindelijk natuurlijk aan elke ondernemer zelf om te kijken wat het risico is op cyberdreiging en om daar ook navenant in te investeren, of dat nou in cyberweerbaarheid, in software of in iets dergelijks is. Dat zal bij een techbedrijf wat meer zijn dan bij een bakker. Voor ondernemers die daar niet zo gevoelig voor zijn, is op veiliginternetten.nl bijvoorbeeld ook software te vinden waar je misschien prima mee uit de voeten kan. Maar het is natuurlijk een kosten-batenafweging. Veiligheid heeft een prijs. Ik denk dat de minister van Justitie en Veiligheid daar goed bij heeft stilgestaan. Die prijs zal waarschijnlijk ook hoger worden. Van overheidswege is er ook maar zoveel wat we kunnen doen. Ik denk dus dat dit een wisselwerking is tussen de eigen verantwoordelijkheid van de ondernemers voor de investeringen die zij doen en de tools die we aanbieden via de website die ik net heb genoemd.

Voorzitter. Ik ga door met de vraag van mevrouw Kathmann over de manier waarop het kabinet via het Digital Trust Center bedrijven geïnformeerd heeft over het bestaan en het nut van digitale hulpverleners, dhv'ers. Bedrijven moeten uiteraard zelf kunnen bepalen op welke manier ze hun digitale hulpverlening inrichten. Dit kan bijvoorbeeld intern of juist extern geregeld zijn. Dat laatste zien we vaak, bijvoorbeeld via een IT-dienstverlener. Het DTC biedt op zijn website informatie over en tools aan voor de manieren waarop bedrijven digitale hulpverlening in hun organisatie kunnen vormgeven. Ook communiceert het DTC actief via samenwerkingsverbanden en socialmediakanalen over het thema digitale hulpverlening. Het Centraal Bureau voor de Statistiek onderzoekt in algemene zin hoeveel bedrijven digitale hulpverlening hebben ingericht en op welke manier ze dat hebben gedaan. De CBS-monitor van 2024 wordt naar verwachting in maart gepubliceerd. Dat wordt een mooi inzicht om te hebben.

Voorzitter. Ik blijf bij mevrouw Kathmann. Zij vroeg mij wat er bij de overheid al aan dhv'ers is gebeurd. Dat ligt op het terrein van mijn collega, de staatssecretaris van BZK. Ik weet dat er enkele voorbeelden zijn van digitale hulpverleners, bijvoorbeeld bij gemeenten. De gemeente Purmerend is daarvan een voorbeeld. Zij richt haar digitale hulpverleners op ondernemers binnen de eigen gemeentegrenzen. Dat kan natuurlijk ook: hulp vanuit de gemeente aan ondernemers binnen de gemeente. Binnen de overheid zelf kennen we verschillende rollen die vanuit hun expertise ondersteuning bieden aan overheidsmedewerkers. Denk onder meer aan de beveiligingsambtenaren binnen de ministeries en de Chief Information Security Officers, waar de minister van JenV al aan refereerde. Daarnaast bestaan natuurlijk ook de Computer Security Incident Response Teams en de Informatiebeveiligingsdienst, de IBD, voor gemeenten. Zij kunnen hulp en ondersteuning bieden aan overheidsorganisaties bij incidenten.

Voorzitter, met uw goedvinden ga ik door naar het volgende blokje, over keurmerken. Ik begin met de vraag van mevrouw Michon-Derkzen over cybersecuritydienstverlening. Dat is booming business. Het is goed om zelf te werken aan kwaliteitsstandaarden, bijvoorbeeld door middel van een keurmerk. Mijn collega van BZK is primair verantwoordelijk voor het aanbestedingsbeleid van de overheid, maar ik kan daar wel het volgende over zeggen. Waar dat relevant is, kunnen keurmerken of de onderliggende eisen vanuit die keurmerken onderdeel zijn van de aanbesteding. Het is momenteel niet mogelijk om in een aanbesteding één specifiek keurmerk voor te schrijven. De mate waarin certificeringseisen en keurmerken worden meegestuurd in de aanbesteding is afhankelijk van het resultaat van een risicoanalyse.

De heer Valize vroeg mij welke acties ondernomen worden om verwarring tegen te gaan tussen de CE-markering en het China Export-logo. Dat is een begrijpelijke vraag. Ondanks dat de toezegging aan de heer Valize destijds niet is geregistreerd, heeft mijn voorganger dit wel voortvarend opgepakt en ook geadresseerd bij de Europese Commissie. Het eerlijke verhaal is dat het complex is, want het aanpassen van het Europese logo neemt niet weg dat China het logo eveneens zou kunnen aanpassen. Het blijft dus lastig te doorbreken. Ik zal dit bij de aankomende Raad Concurrentievermogen van 6 maart nogmaals onder de aandacht brengen. Ik kan toezeggen dat de updates, zoals die zojuist zijn toegelicht, en de mogelijke aanvulling naar aanleiding van het opbrengen in Europees verband voor het meireces met uw Kamer gedeeld worden.

Ik blijf bij de heer Valize. Hij vroeg naar de motie en het keurmerk voor ICT-dienstverleners ten behoeve van het mkb. Het keurmerk voor ICT-dienstverleners is een marktinitiatief in Nederland. Dat maakt het echt onderscheidend. Het keurmerk wordt getrokken door het Centrum voor Criminaliteitspreventie en Veiligheid, het CCV. Dit centrum zal het keurmerk beheren en uitgeven. Dat sluit ook aan bij de intentie van de motie-Rajkowski, die pleit voor de ontwikkeling van een eenduidig mkb-keurmerk in samenwerking met het DTC en de relevante brancheorganisaties. Dit keurmerk moet mkb'ers effectief ondersteunen bij het vormgeven van hun securitybeleid. Daarmee is het onderscheidend van het CE-merk. Het CE-merk is voorbehouden aan het Europese wettelijke systeem van productregulering.

Voorzitter. Ik ben aangekomen bij het kopje innovatie in het onderwijs en cybersecurity. Mevrouw Michon-Derkzen vroeg of de agenda Cybersecurity Technologies onderdeel is van de Nederlandse Cybersecuritystrategie. Het antwoord daarop is ja. Onder pijler II

van de Nederlandse Cybersecuritystrategie is de doelstelling opgenomen om een sterke cybersecuritykennis- en innovatieketen in Nederland te ontwikkelen. Daarmee is het ook een belangrijk speerpunt onder de NLCS. Deze doelstelling is nader uitgewerkt in de agenda Cybersecurity Technologies onder de Nationale Technologiestrategie, waarbij cybersecurity is aangemerkt als een van de tien prioritaire technologieën, die u welbekend zijn. Ze sluiten daarom ook naadloos op elkaar aan. De agenda Cybersecurity Technologies is op 7 juni 2024 naar de Kamer gestuurd. Samen met Nederlandse marktpartijen, kennisinstellingen en ecosysteempartners wordt toegewerkt naar een meer concrete actieagenda. De voortgang van dit proces wordt in het derde kwartaal van dit jaar met uw Kamer gedeeld.

Mevrouw Kathmann vroeg hoe de ministers samen optrekken in het kader van een stevige agenda voor het opleiden van personeel. Dat is een goede vraag. Dank daarvoor. In het najaar van 2024 is onder het bestaande programma van de Human Capital Agenda ICT een programmalijn opgezet voor cybersecurity. Binnen deze programmalijn is een taskforce opgericht die bestaat uit vertegenwoordigers van het Nederlandse bedrijfsleven, universiteiten, hogescholen, mbo-instellingen en de overheid. Dat is dus een heel rond spectrum. Samen met alle leden van de taskforce zijn vier prioritaire thema's bepaald, die in het komende jaar verder worden uitgewerkt via werktafels. Het opleiden van personeel wordt hierin uiteraard meegenomen. Ook de ministeries van Binnenlandse Zaken, Justitie en Veiligheid, en Onderwijs, Cultuur en Wetenschap zijn hierbij betrokken.

Voorzitter. Ik ben aangekomen bij het kopje overig. Het lid Six Dijkstra en het lid Kathmann vroegen of wij bekend zijn met ondernemers die een IT-jaarverslag gebruiken. Ik ben uiteraard bekend met het NOREA Reporting Initiative. Mij is ook ter ore gekomen dat diverse bedrijven heel positief zijn over het NRI. Zij beschouwen het als een innovatieve en complete reporting tool. Een voordeel van het NRI is dat het op een eenduidige en holistische wijze inzicht geeft in de kwaliteit en betrouwbaarheid van de IT-beheersing. Het introduceert daarmee ook een soort gestandaardiseerde aanpak voor IT-rapportages. Dat is heel positief. Stakeholders krijgen daarmee een helder inzicht in en overzicht van hun aanpak ten aanzien van cruciale IT-thema's, zoals cybersecurity, datagovernance en IT-continuïteit. Het NRI integreert daarmee bestaande wettelijke en compliance-eisen, waardoor de versnippering in audit- en toezichtprocessen wordt verminderd en organisaties efficiënter kunnen voldoen aan de regelgeving. In die zin ben ik blij dat het NRI daarmee bijdraagt aan een andere prioriteit van Economische Zaken, namelijk het verminderen van de regeldruk.

Ik heb nog een vraag gekregen van mevrouw Koekkoek over zeekabels. Kan ik uitleggen wat we doen om het risico op sabotage te verminderen? Die vraag leeft heel duidelijk, want ik heb dit antwoord al in meerdere commissies mogen geven. In het Programma Bescherming Noordzee Infrastructuur werkt het kabinet aan verschillende maatregelen om de sabotage van onderzeese infrastructuur te voorkomen, zoals een versterking van de beeldopbouw. De Kustwacht intensiveert de patrouilles en werkt aan het verbeteren van de sensorische systemen. Er is ook een uitbreiding van de Defensiecapaciteit. Het ministerie van Defensie bouwt extra capaciteiten, onder andere met drones en patrouillevaartuigen. Er is ook sprake van internationale samenwerking. Nederland werkt samen met bondgenoten om de beveiliging van de kritieke infrastructuur op zee te verbeteren. Dat omvat gezamenlijke oefeningen en kennisdeling. Denk ook aan de informatievoorziening en informatiedeling. De Tweede Kamer wordt

middels Kamerbrieven op de hoogte gehouden van de voortgangsrapportages en het actieplan van het PBNI. In de vorige Telecomraad heb ik dit ook te berde gebracht en heb ik met de Zweedse en Finse counterparts gesproken over kabels. Dat gebeurt daar wat dichter bij huis dan hier. Ook daar is dus sprake van een overdracht van kennis en informatie hierover.

Ik ben aangekomen bij de vraag van mevrouw Michon-Derkzen over de reactie van het kabinet op de oproep tot het faciliteren van gegevensdeling voor de helpdesk inzake onlinebankfraude. De telecomproviders spelen een belangrijke rol bij de aanpak van onlinefraude. Er wordt, zoals u weet, regelmatig misbruik gemaakt van telecomvoorzieningen. Het huidige wettelijke kader in de Telecommunicatiewet biedt maar beperkte ruimte voor de aanpak van onlinefraude. Net als de sector zie ik daarom ruimte voor verbetering. Ik onderzoek dan ook of we kunnen komen tot een passende grondslag voor het verwerken van verkeersgegevens in de Telecommunicatiewet. Dat is nodig om gegevensdeling mogelijk te maken voor de aanpak van online fraude. Daarbij hecht ik ook groot belang aan goede privacywaarborgen. Daarnaast ben ik bezig met een aanpassing van de Telecommunicatiewet die gericht is op het voorkomen van misbruik van nummers, bijvoorbeeld voor phishing en spoofing. Ik wil deze voorstellen zo veel mogelijk afstemmen met de ontwikkeling van Europese regels, waaronder ook de payment services regulation. De wijzigingen in de Telecommunicatiewet beogen overigens vooral een preventieve werking. Dat is dus ook in aanvulling op de strafrechtelijke aanpak van misbruik en fraude.

Mevrouw **Michon-Derkzen** (VVD):
Ik hoor de minister zeggen "wij onderzoeken een passende grondslag" en "we wachten ook op Europa". Ik zou hem willen vragen wanneer er een wijziging van de Telecommunicatiewet voorzien is waar dit in meegenomen zou kunnen worden. Als de minister het niet doet, doen we het per amendement. Wanneer kunnen we dus een wijziging van de Telecommunicatiewet verwachten?

Minister **Beljaarts**:
Dank voor de vraag. Dat is een terechte vraag. Vanuit de verantwoordelijkheid van de Kamer is dit een hele goede vraag. U weet hoe stroperig dit kan zijn. Ik kan mevrouw Michon-Derkzen comfort bieden met een voortgangsbrief waarin ik uitgebreid terugkom op de timing. Dan maken we inzichtelijk wat de eerstvolgende mogelijkheid is om met een aanpassing van de Telecommunicatiewet aan de slag te gaan. Ik hoop dat ik daarmee comfort bied, want het is een terechte vraag en daar wil ik graag zorgvuldig antwoord op geven.

De **voorzitter**:
U vraagt om een bevestiging. Nog een verhelderende toelichting van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Los van de roep uit de sector, die een wijziging van de Telecommunicatiewet nodig heeft om die bankhelpdeskfraude beter aan te kunnen pakken — ik heb het niet verzonnen; dat hebben ze zelf verzonnen — hoor ik de minister zeggen dat er überhaupt een wijziging van deze wet aanstaande is. Mijn vraag is dus — ik zit daar namelijk niet in — wanneer de wijziging van de Telecommunicatiewet naar de Kamer komt.

Minister **Beljaarts**:
Dank voor de vraag. Het is geen procesantwoord in de trant van "we kijken ernaar en we komen erop terug". Dit is echt een actueel onderwerp waar we daadwerkelijk hard aan werken. Er is nu nog geen harde deadline wanneer dit komt. We zijn namelijk ook op Europees vlak aan het kijken wat er al loopt en of we daarop aan kunnen sluiten. Daarom stel ik voor om binnen twee weken met een voortgangsbrief te komen om daar meer inzicht in te geven, zodat mevrouw Michon-Derkzen er comfort bij heeft dat we er daadwerkelijk voortvarend mee aan de slag gaan. Ik weet dat we dat comfort met 99% zekerheid kunnen geven. Als u daarmee akkoord gaat, dan doe ik dat met plezier.

De **voorzitter**:
Akkoord. Dan mag u uw bijdrage continueren.

Minister **Beljaarts**:
Dank. Ik was aan het einde gekomen, maar ik had nog twee nagekomen berichten, deels via de minister van JenV en deels rechtstreeks via mevrouw Koekkoek van Volt. Dat ging onder andere over het informeren en het in beweging zetten van het mkb, het bedrijfsleven, als het gaat om het kwantumtijdperk. Dat wilde ik zeker niet voorbij laten gaan, want dat is natuurlijk een heel belangrijk onderwerp. Zoals eerder ook aangegeven, doet het Digital Trust Center aan voorlichting, onder andere via websites, socialmediaplatforms en de keten. Maar het Post-quantumcryptografiemigratiehandboek — dat is een hele mond vol, maar het bestaat — van BZK en de AIVD is gericht op de overheid, maar is ook relevant voor het bedrijfsleven. Er is gewoon informatie beschikbaar waar je je voordeel mee kan doen.

Om iets dieper antwoord te geven op het gebied van bijvoorbeeld AI: er loopt een initiatief vanuit mij, in samenwerking met andere Europese landen, om te kijken hoe we onder andere AI onder de Digital Markets Act kunnen brengen, om daar dus ook wat meer toezicht en grip op te houden. Ik hoop dat het comfort biedt dat we daadwerkelijk stappen aan het nemen zijn, ook op het gebied van kwantum, zoals AI.

Mevrouw Koekkoek vroeg ook: hoe gaat het met de implementatie van de wetgeving en het DTC? Ze vroeg met name naar de impact die we daarvan verwachten voor het mkb. We doen daar al veel. Ik noem bijvoorbeeld de wet die betrekking heeft op het DTC, de rechtsgrondslag om informatie te kunnen delen, de subsidie vanuit het DTC om bedrijven te helpen, de ondersteuning bij de implementatie van de Cyber Resiliance Act en de financiële steun voor het mkb.

Dan ben ik aan het einde gekomen van de beantwoording.

De **voorzitter**:
Ik zie geen interrupties. Ik dank u voor de beantwoording. Dan ga ik meteen door naar de tweede termijn van de zijde van de Kamer, beginnend bij de heer Six Dijkstra namens Nieuw Sociaal Contract.

De heer **Six Dijkstra** (NSC):
Dank, voorzitter. Ik vond dit zelf een goed debat. Heel veel onderwerpen zijn de revue gepasseerd. Beide ministers hebben samen al mijn vragen beantwoord, dus dank daarvoor. Ik heb ook geen verdere vragen. Ik wil de leden van de commissie bedanken voor het goede en inhoudelijke debat.

De **voorzitter**:
Heel hartelijk dank. Ik zie geen interrupties, dus ik denk dat iedereen het ermee eens is. Dan geef ik het woord aan mevrouw Michon-Derkzen. Zij spreekt namens de Volkspartij voor Vrijheid en Democratie.

Mevrouw **Michon-Derkzen** (VVD):
Dank, voorzitter. Ik dank ook beide bewindspersonen voor de beantwoording. Het is heel goed dat we het vandaag over dit eigenlijk veelomvattende onderwerp hebben. Dat zie je wel aan alle vragen die langskomen.

Ik wil nog op een paar dingen de aandacht vestigen, bijvoorbeeld op de noodzaak van bewustwording bij mensen thuis. Ik ken zelf bijvoorbeeld het programma Black-out van de EO niet; dat ga ik zeker nog proberen te kijken. Ik zou de minister van JenV willen vragen of hij dit soort initiatieven kan onderzoeken en of hij daar wellicht op kan intensiveren, zodat we die bewustwording vergroten. Dan over rapid response en de verdringing van die prioritaire bijstand. Als er tegelijkertijd van alles misgaat, hoor ik de minister zeggen dat er voor de vitale sectoren een afwegingskader is als bijlage van het Landelijke Crisisplan Digitaal. Dat kan ik goed volgen, maar mijn punt is vooral dat die aansturing dan per definitie publiek-privaat is. Ga je als minister bijvoorbeeld over een academisch ziekenhuis? Nee, dat is privaat. De vraag is dus hoe die aansturing in crisissituaties gaat. Ik vind dat eigenlijk een hele spannende vraag, waarvan ik denk: hebben we dat nou goed op orde? Dat zag je ook in de coronatijd. Eigenlijk is een digitale crisis per definitie publiek-privaat. Die zal zich nooit alleen tot publieke organisaties beperken. Dat afwegingskader stelt me gerust. Ik hoef het overigens niet als "vertrouwelijk" te zien, want wat heb ik daaraan? Maar ik zou over die aansturing nog wel graag wat meer informatie willen.

Ook wil ik graag nog wat meer informatie over die beperkingen die wij aan Europese aanbestedingen kunnen stellen, maar ik denk dat ik daarvoor bij BZK moet zijn. Ik vind namelijk dat je een keurmerk wel degelijk als basis moet proberen in te zetten, omdat je een minimale kwaliteitsstandaard wil. Ook qua bescherming en weerbaarheid heb ik nog wel een aantal punten waarmee je via Europese aanbestedingen wat steviger moet sturen op het beschermen van je economie. Dat is nodig voor onze veiligheid. Dat druist ook in tegen mijn hele DNA, maar het is niet anders; we zitten ermee.

Dan dank ik de minister van EZ voor zijn toezegging van een brief over die bankhelpdeskfraude. Ik wil graag een tweeminutendebat aanvragen, voorzitter. In afwachting van de brief kijk ik hoe ik daar verder mee omga.

Dat geldt ook voor het volgende punt, zeg ik tegen de collega's, voordat ze denken: wat wil ze allemaal? Ik denk dat het ook goed is dat de Kamer een uitspraak doet over het wel of niet laten vallen van het hoger onderwijs onder die NIS2. Omdat het zo'n groot project is, vind ik dat we daar met z'n allen in het begin aan mee moeten doen. Ook dat zou je niet moeten willen, maar we zitten in mijn ogen niet meer in de luxepositie. We lopen ook een risico met ons hoger onderwijs en onze cybersecurity.

Daar laat ik het bij.

De **voorzitter**:

Hartelijk dank voor uw bijdrage in de tweede termijn. Ik zie geen interrupties, dus we kunnen meteen door naar mevrouw Koekkoek, die namens Volt haar inbreng in de tweede termijn zal doen.

Mevrouw **Koekkoek** (Volt):
Dank, voorzitter. Dank voor het goede debat. Dank aan de bewindspersonen en zeker ook aan de ondersteuning voor de beantwoording. Ik sluit me aan bij de vragen van collega Michon over de weerbaarheid. Ik vond het wel mooi om te horen dat er een soort wedstrijdje speelt tussen landen over wie het meest weerbaar is. Ik denk dat dat op zich een positieve ontwikkeling is en dat Nederlanders zeker nog wel een been bij kunnen trekken. Als overheid kun je daar nog wel wat meer op sturen, juist op het gebied van cyber. Je hebt de fysieke dreiging, maar zeker ook de digitale dreiging.

Voorzitter. Op twee dingen wil ik nog even doorvragen. We hebben het gehad over de impact op het mkb. Daar zijn we uitgebreid op ingegaan. Ik zou dezelfde vraag willen stellen over de impact op start-ups. Kan de hoeveelheid regels een belemmering zijn voor een start-up om überhaupt verder te komen? Maar het geldt ook andersom. Als er cyberincidenten zijn, is dat voor start-ups een belemmering om op te schalen. Ik zou graag van de minister willen horen in hoeverre dat een probleem is en wat we daar specifiek voor kunnen doen, want het mkb is net weer iets anders dan start-ups. Ik kan me ook voorstellen dat daarvoor andere ondersteuning nodig is.

Het tweede waar ik op door wil vragen, betreft kwantum. Ik denk dat het ontzettend goed is dat het al scherp staat. Dank voor de toezegging om het in het oog te houden en erover na te denken. Het is ook een goede ontwikkeling dat AI onder de DMA wordt gebracht, denk ik. Daar zie ik ook positieve ontwikkelingen. Deel één van het verhaal is eigenlijk dat je als overheid kijkt of bedrijven het goed doen en ze daarbij ondersteunt. Maar deel twee zou moeten zijn dat je ook in de smiezen kan houden of het goed loopt. Daar zit een beetje mijn zorg, die ik al eerder aanstipte. Moeten we als overheid misschien op een gegeven moment extra bijsturen? Het gaat er niet per se om om dingen op te leggen, maar op Q-day, Q-dag, moet je wel zeker weten dat het goed staat. Ik wil zelf voorkomen dat we krijgen wat we nu bij cyberdreigingen zien. Als overheid waren we in eerste instantie scherper op statelijke actoren, maar je zag dat bedrijven daardoor wel kwetsbaar waren. Het lijkt me voor iedereen negatief, voor bedrijven maar zeker ook voor de maatschappij als geheel, als je dat straks bij kwantum ook ziet. De concrete vraag die ik wil stellen, is: hoe kunnen we dat nu een beetje scherp houden? De minister gaf wel aan dat hij het in de smiezen houdt, maar kunnen we er ook een manier voor vinden om overzicht te houden? Een voortgangsrapportage is hierbij misschien een gek woord. Het gaat erom dat de Kamer ook kan meekijken, dus dat je, op het moment dat je een beetje bij moet trekken, dat ook echt kan doen.

Dank, voorzitter.

De **voorzitter**:
Heel hartelijk dank, mevrouw Koekkoek. Ik zie geen interrupties, dus we kunnen meteen door naar mevrouw Kathmann namens GroenLinks-PvdA voor haar tweede termijn.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dank, voorzitter. Ook ik wil de ministers bedanken voor hun beantwoording en dit debat. Er moet me wel echt iets van het hart. We hadden het even over de

cyberweerbaarheidskloof, maar ik vind dat ook is blootgelegd welke kloof er is tussen dit kabinet en mensen met een kleine beurs. Ik heb even een kleine optelsom gemaakt. Die loopt gewoon op tot €1.000 per jaar. Dan heb je niet eens de basics op orde. Dan heb je het alleen al over het verschil tussen een veilige telefoon en een heel goedkoop, knetteronveilig telefoontje, over veilige providerspakketten of gewoon een veilig softwarepakket en over maar één betaalde app, in plaats van een gratis app. €1.000. Kleine ondernemers met nagenoeg geen investeringsruimte zijn al snel €10.000 kwijt. Er is niet gevraagd om zakken en bakken met geld uit te geven om deze mensen te helpen, maar alleen maar om centraal te informeren. Dat was de vraag. Daar wil ik het niet eens over hebben, maar het moest me gewoon heel erg van het hart.

Ik wil het nog even hebben over een ander veiligheidsvraagstuk. Het werd gelukkig door iedereen hier gedeeld. Het is echt van wezenlijk belang. De Nederlandse veiligheid is ook belangrijk voor onze buurlanden en eigenlijk voor heel Europa, voor al onze partners natuurlijk. Daarin speelt end-to-endversleuteling echt een heel belangrijke rol. We hebben er natuurlijk al een heel uitgebreid debat over gehad, omdat er een Europees voorstel op tafel ligt. Er ligt binnenkort weer een voorstel op tafel dat hierover gaat, en dan expliciet over het wel of niet inbouwen van een scan om chatapplicaties in heel Europa te scannen. Weet de minister op welke termijn Polen dat voorstel weer op tafel gaat leggen? Heeft de minister al een nieuw voorstel gezien? Wordt de Kamer deze keer op tijd geïnformeerd? De vorige keer hebben we het namelijk eigenlijk alleen maar via de achterkamertjes vernomen. Werkt de minister in de voorbereiding al samen met partijen, al onze experts, zoals Offlimits en de ATKM? De allerbelangrijkste vraag is natuurlijk: kunnen we er weer van op aan dat encryptie overeind blijft, zowel in Nederland als in Europa?

De **voorzitter**:
Dan dank ik u voor uw tweede termijn. Ik zie geen interrupties. Ik draag heel even het voorzitterschap weer over aan de heer Six Dijkstra, zodat ik zelf mijn tweede termijn kan doen.

Voorzitter: Six Dijkstra

De **voorzitter**:
Dank u wel. Bij dezen het woord aan de heer Valize voor zijn tweede termijn.

De heer **Valize** (PVV):
Voorzitter, hartelijk dank voor het woord. Dank aan iedereen voor het constructieve debat. Ik heb heel wat voorbij horen komen, maar ik sluit me toch aan bij het laatste stukje van mevrouw Kathmann, met betrekking tot de end-to-endencryptie. Die moet echt overeind blijven. Het kan niet zo zijn dat wij dadelijk voor ons communicatienetwerk die end-to-endencryptie gaan opheffen, alleen maar om het doorzoekbaar te houden of in ieder geval er potentieel iets uit te filteren. Dat kan niet de bedoeling zijn, dat mag niet en dat moet niet. Dat zal never nooit niet mogen gebeuren. Ik hoop dat die oproep ook bij het kabinet is aangekomen. We hebben daarover inderdaad met z'n allen een brief ontvangen.

Voor de rest wil ik even terugblikken op het debat. Ik wil iedereen danken voor de beantwoording: de minister van Economische Zaken en de minister van Justitie en Veiligheid. Volgens mij zijn al mijn vragen beantwoord. Bij de laatste vraag dreigde ik

met een motie te komen. Die motie hoef ik niet in te dienen, want ik heb een mooie toezegging gekregen. Minister Beljaarts zal het meenemen naar de Raad Concurrentievermogen die gepland staat op 5 maart. Dit komt dan weer terug bij Economische Zaken; ik zal mijn collega heel lief aankijken, net zo vriendelijk als ik hier in de commissie probeer te doen. We zullen er in ieder geval bovenop blijven zitten.

Voor de rest dank ik iedereen voor dit constructieve debat.

De **voorzitter**:
Dank u wel voor uw inbreng, meneer Valize. Bij dezen geef ik de voorzittershamer weer aan u terug.

Voorzitter: Valize

De **voorzitter**:
Hartelijk dank voor het tijdelijk voorzitterschap, de heer Six Dijkstra. Ik kijk even naar de rechterzijde. Dient er nog geschorst te worden, of kan iedereen meteen overgaan tot de beantwoording? Dat laatste is het geval. Dan geef ik het woord aan de heer Van Weel, minister van Justitie en Veiligheid.

Minister **Van Weel**:
Dank, voorzitter. Grofweg zijn er twee hoofdvragen van vier leden. De eerste vragen, van mevrouw Michon en mevrouw Koekkoek, gingen over weerbaarheid en het vergroten daarvan. Ja, we staan aan het begin van dit traject. Die race binnen Europa willen we natuurlijk winnen door onze weerbaarheid naar het hoogste plan te brengen. Er komt in het voorjaar ook een campagne over weerbaarheid. Daar kunt u dus op wachten. Natuurlijk zullen we dit ook in het digitale domein meenemen. Zoals ik al zei spreken we op 10 april ook over dit onderwerp, maar dan ook met de minister van Defensie erbij.

De tweede set vragen kwam van mevrouw Kathmann en de heer Valize. Deze vragen ging over het voorstel dat eind vorig jaar voorlag in de JBZ-Raad en het toen niet heeft gehaald. Het is ook niet formeel ingediend. Daar hebben we uitgebreid over gesproken met uw Kamer. Uw Kamer heeft daar een aantal voorwaarden aan gesteld. Die voorwaarden acht ik nog steeds als leidend bij de beoordeling van nieuwe voorstellen die binnenkomen. Ik weet dat het Poolse voorzitterschap nu broedt op de vraag of en, zo ja, op welke wijze dit verder moet worden opgepakt. Ik verwacht dat we aanstonds een eerste voorstel zullen zien. Zoals we dat altijd doen bij de voorbereiding van een JBZ-Raad nemen we uw Kamer mee in waar die voorstellen op zien en waar wij als kabinet voornemens zijn om mee in te stemmen.

De **voorzitter**:
Ik zie een interruptie. Wie was eerst, mevrouw Michon-Derkzen of mevrouw Kathmann? Mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Is "aanstonds" iets meer in te vullen? Betekent dat binnenkort, of valt daar nog weinig over te zeggen? Ik ben daar gewoon benieuwd naar.

Minister **Van Weel**:

Als u "binnenkort" specifieker vindt dan "aanstonds", dan kan ik mij ook in "binnenkort" vinden. Inderdaad, mevrouw Kathmann, een paar maanden. Ik weet niet of dat al eind maart in de JBZ-Raad voorligt, maar anders zal het zeker de JBZ-Raad daarna zijn. Het ligt ook een beetje aan de route die het voorzitterschap wenst te nemen, of dat een hele simpele verbouwing wordt of een grote verbouwing. In het laatste geval zal het wellicht langer moeten duren.

De **voorzitter**:
Dan had u ook nog een interruptie van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Ja. Ik mis een antwoord op de vraag over de aansturing bij een cyberaanval die zowel publieke als private doelen raakt. Het afwegingskader bij "vitaal" snap ik, maar hoe ziet de aansturing eruit als ook publieke en private doelen zijn geraakt?

Minister **Van Weel**:
Mevrouw Michon heeft helemaal gelijk. Excuses voor de omissie. In het derde kwartaal van dit jaar komen we met een handboek naar aanleiding van het Landelijk Crisisplan Digitaal. Dat handboek lost ook deze aansturingsvraagstukken op. Dat is per sector verschillend. Soms is er sprake van een doorzettingsmacht. In andere sectoren is het meer een coöperatie. Soms is het ondersteuning. Dat handboek gaat daar helderheid in brengen.

De **voorzitter**:
Dan zie ik geen verdere interrupties en dank ik de heer Van Weel voor zijn bijdrage. We gaan door naar de minister van Economische Zaken, de heer Beljaarts.

Minister **Beljaarts**:
Dank u, voorzitter. Ik begin met een aanvulling op de zorg van mevrouw Michon-Derkzen over weerbaarheid. Wij zijn heel actief met weerbaarheid voor het bedrijfsleven. Dat doen we natuurlijk in nauw overleg met de ministers van JenV en Defensie en met de inzichten van de diensten, om te zorgen dat het bedrijfsleven weerbaarder wordt, zonder paniek te zaaien, maar wel om de juiste sense of urgency te laten landen bij bedrijven. Daar wordt met de brancheverenigingen druk op gehandeld om te zorgen dat die awareness er is en dat men snapt wat je doet als je wat langer zonder stroom zit, misschien een paar dagen, als er fysieke sabotage is, als je geen internet hebt en geen pinbetalingen meer kunt doen et cetera. Daar wordt dus hard aan gewerkt.

De tweede opmerking van mevrouw Michon-Derkzen ging over het keurmerk en overheidsaanbestedingen. Ik heb daar in andere commissies ook vragen over gekregen. Ik neem dit ook mee naar collega-staatssecretaris Szabó, omdat er meerdere wensen zijn als het gaat om aanbesteden, zoals duurzaam aanbesteden, het aanbesteden van EU-bedrijven, ook als het gaat om clouddiensten, en misschien soms het bevoordelen van start-ups. Er zijn heel veel wensen. Ik neem die mee. Wees gerust dat ik die vragen zal doorgeleiden en ook zal opvolgen.

Mevrouw Koekkoek vraagt specifiek naar start-ups. Ik zie niet zo heel specifiek het verschil tussen het dreigingsbeeld bij mkb en bij start-ups. Uiteraard worden start-ups ook meegenomen in de advisering van het Digital Trust Center, maar er is bij start-ups niet een specifiek beeld dat afwijkt ten opzichte van mkb-bedrijven. Sommige start-ups

zijn eigenlijk mkb-bedrijven en vallen dus al onder die paraplu. Dat zie ik dus niet. Ook start-ups kunnen natuurlijk altijd terecht bij het Digital Trust Center.

Dan denk ik alle vragen beantwoord te hebben, voorzitter. Dank.

De **voorzitter**:
Dan dank ik minister Beljaarts voor de beantwoording. Ik kijk naar de linkerzijde. Ik zie geen interrupties, dus alle vragen zijn beantwoord. Ik zal nog even kort recapituleren wat er zoal aan toezeggingen is gedaan.

Het lid Michon-Derkzen vraagt een tweeminutendebat aan. Daar zal zij de eerste spreker zijn. Dit zal worden doorgeleid naar plenair om te worden ingepland.

- Dan hebben wij een toezegging van de minister van Justitie en Veiligheid dat burgerbetrokkenheid betrokken zal worden bij de uitwerking van het vernieuwde plan over weerbaarheid, dat naar verwachting in het voorjaar van 2025 met de Kamer zal worden gedeeld. Dit naar aanleiding van de vraag van de heer Six Dijkstra.

Ik zie geknik, dus dat klopt.

- Er is een toezegging van de minister van Economische Zaken dat bij de volgende Raad Concurrentievermogen het probleem omtrent de mogelijke verwarring bij keurmerken, bijvoorbeeld tussen de CE-markering en het China Export-logo, onder de aandacht zal worden gebracht en dat naar aanleiding hiervan voor het meireces 2025 met de Kamer een update zal worden gedeeld. Dit naar aanleiding van de vraag van het lid Valize.

Dat klopt, zie ik.

- Dan hebben we nog een laatste toezegging. De minister van Economische Zaken zegt toe de Kamer middels een voortgangsbrief binnen twee weken te informeren over de planning van wijzigingen in de Telecommunicatiewet. Dit naar aanleiding van de vraag van het lid Michon-Derkzen over bankhelpdeskfraude.

Dat klopt allemaal? Ja? Dan zijn wij niets vergeten.

Ik geef de kijkers thuis en de mensen op de tribune nog even mee dat zij, als zij willen weten wat zij zelf aan weerbaarheid kunnen doen, altijd de website veiliginternet.nl kunnen raadplegen. Op de website van het DTC, Digital Trust Center, kunnen de mkb'ers handreikingen raadplegen. En dan hebben we ook nog een hele leuke kijkerstip gekregen van de heer Van Weel met betrekking tot het preppen: het programma is van de Evangelische Omroep en is getiteld Black-out. We kunnen dat waarschijnlijk terugkijken op de app van NPO. Ik dank iedereen voor het mooie en waardige debat.

Sluiting 15.43 uur.