2
Vragenuur: Vragen Eerdmans

Aan de orde is **het mondelinge vragenuur**, overeenkomstig artikel 12.3 van het Reglement van Orde.

Vragen van het lid Eerdmans aan de minister van Justitie en Veiligheid over **het bericht dat miljoenen zonnepaneelinstallaties in Nederland door slechte cybersecurity gemakkelijk te hacken zijn**.

De **voorzitter**:
Aan de orde is het mondelinge vragenuur. Ik heet de minister van Justitie en Veiligheid, de woordvoerders, de mensen op de publieke tribune en de mensen die op een andere manier het vragenuur volgen van harte welkom. Ik geef als eerste het woord aan de heer Eerdmans van JA21. Hij heeft een mondelinge vraag aan de minister over het bericht dat miljoenen zonnepaneelinstallaties in Nederland door slechte cybersecurity gemakkelijk te hacken zijn. Het woord is aan de heer Eerdmans van JA21.

☐

De heer **Eerdmans** (JA21):
Voorzitter, dank u zeer. We hebben in Nederland een waakhond die onze digitale infrastructuur moet bewaken. Die waakhond slaat vandaag in een rapport alarm. Dit is niet zomaar iets. Het blijkt dat onder andere zonnepaneelinstallaties — we hebben daar miljoenen van in Nederland, 16 miljoen installaties heb ik gelezen — vrij gemakkelijk gehackt kunnen worden. Daar zit weinig bescherming omheen. Niet een van de geteste apparaten voldeed aan de veiligheidseisen van de inspectie. Dit kan natuurlijk nare gevolgen hebben voor mensen met een zonnepaneel op het dak. Als hackers over al die zonnepanelen tegelijk controle zouden krijgen kan dit zelfs nog veel naardere gevolgen hebben. Dan kunnen ze samen namelijk ingezet worden als een ddos-aanval op onze totale digitale infrastructuur. In dat geval gaat alles plat. We hebben het dan over het luchtverkeer, over het scheepvaartverkeer en over C2000-masten. Dit is volgens de inspectie een reëel scenario. Wij delen die zorgen. Ik denk dat de minister deze zorgen ook deelt; ik zie haar nu al knikken. Deelt u ook de analyse van de RDI die hier onderligt? De enorme kwetsbaarheid van de slimme apparaten die wij thuis hebben. Dit zijn er natuurlijk veel meer dan alleen de zonnepanelen. Bent u zich daarvan bewust? Bent u er zich ook van bewust dat heel veel mensen in ons land daar juist helemaal niet mee bezig zijn? Dat mensen dat ook niet controleren en daar zich het gevaar niet van realiseren? Dat kun je ze ook nauwelijks kwalijk nemen. Wat gaat u daaraan doen? Laat ik met deze twee vragen openen.

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

☐

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Bedankt ook voor deze vragen. Ik ben zeker bekend met het Telegraaf-artikel. In dit artikel wordt ook gesproken over miljoenen zonnepaneelinstallaties in Nederland die door slechte cybersecurity makkelijk te hacken zijn. Het bericht, dat ook over andere apparatuur gaat, nemen wij uiterst serieus. De Nationaal Coördinator Terrorismebestrijding en Veiligheid publiceert jaarlijks een Cybersecuritybeeld Nederland, waarin nadrukkelijk aandacht wordt gevraagd voor de toenemende digitale dreiging. Vanuit het kabinet zetten wij ons ervoor in om te voorkomen dat deze risico's een bedreiging vormen voor de continuïteit, integriteit en vertrouwelijkheid van alle vitale processen in ons land, waaronder energie. Ik doe dat bijvoorbeeld nauw samen met mijn collega van EZK. Ik bouw het heel even op vanuit zonnepanelen, want daar ging het artikel natuurlijk specifiek over. Ik zal zo ook ingaan op de vraag van de heer Eerdmans. Dit betekent dat transport, distributie en productie van elektriciteit op land en op zee door de minister van EZK zijn aangemerkt als vitale processen. Dat is belangrijk, omdat dit betekent dat er dan periodiek analyses plaatsvinden van dreigingen, risico's en het weerbaarheidsniveau. Ook vindt toezicht door een toezichthouder plaats. Dat is natuurlijk ook het bericht van de Rijksinspectie Digitale Infrastructuur. Dat past ook hierbij: een cyclus van monitoring van dreiging en het treffen van passende maatregelen.

Voor huishoudelijke apparatuur en slimme apparatuur die wij in onze huizen kunnen hebben — de heer Eerdmans stelde daar een terechte vraag over — is er specifieke Europese wetgeving in de maak, om ervoor te zorgen dat we mensen voorlichten en informatie geven over hoe met dat soort apparaten om te gaan. Met die wetgeving kunnen we er ook voor zorgen dat het goed geborgd is dat die veiligheidseisen zijn geregeld en zo nodig worden afgedwongen. Het is dus en-en op al die terreinen.

De heer **Eerdmans** (JA21):
Ik kom zo even terug op de wetgeving. Het punt is dit. Alle apparaten die in ons huis aanwezig zijn, zijn in feite al een springplank voor criminelen. Weinig mensen zijn zich daar echt van bewust, denk ik. Er zijn mensen die al alleen met hun iPad of telefoon de lampen aandoen en de thermostaat aan- of uitzetten. Ik noem de slimme meter, de televisie, de bewakingscamera. Hele huizen zijn digitaal bemand. De enige deur die dan voor een crimineel open moet om daar gigantisch misbruik van te maken, is die digitale voordeur. Sterker nog, er wordt grote schade berokkend, ook aan de rest van het land.

U noemt wetgeving. Ik weet dat we feitelijk met een gap van een jaar zitten, totdat Europese regels doordringen en onze telecommunicatiewetseisen daarin worden versterkt. We zitten dus eigenlijk met een jaar overgang. Hoe gaat u daarmee om? Wat moeten we doen om in dat jaar, eigenlijk een tussenjaar, toch onze software te beschermen? En wat doen we richting de fabrikanten? Dat is eigenlijk mijn laatste vraag. Ik begreep uit het onderzoek dat vandaag is uitgekomen, dat heel veel fabrikanten wel zijn gewezen op de gevaren, maar dat zij zich die niet realiseren en dat er pas boetes kunnen worden uitgedeeld nadat wij volgend jaar die wet hebben aangepast. Hoe ziet de minister dat?

Minister **Yeşilgöz-Zegerius**:
Laat ik het zo zeggen: ook nu maken we inderdaad al afspraken met fabrikanten. We gaan niet wachten op wetgeving. We zullen ook zorgen dat onze gesprekken en onze afspraken — die zullen ook uitgaan van bijvoorbeeld EZK en andere partners — dringend zijn. Vervolgens is het heel

erg belangrijk dat de mensen thuis — daarom ben ik extra blij met deze vragen — continu alert zijn op het feit dat de passwords moeten worden ingesteld en elke keer tijdig moeten worden aangepast; dat komt in verschillende debatten van ons altijd terug. Er is dus én een verantwoordelijk van de fabrikant, én er wordt natuurlijk opgetreden vanuit de overheid, zoals met nieuwe wetgeving, maar we moeten ook heel erg wijzen op de verantwoordelijkheid en het handelingsperspectief van de mensen die een apparaat hebben. In afwachting van de verplichtingen voert de rijksinspectie dus ook dringende gesprekken met de producenten en importeurs van deze apparaten. Het gaat erom dat aan hen duidelijk gemaakt wordt dat zij moeten handelen, dat we niet gaan wachten op wetgeving. We blijven ook inzetten op die bewustwordingscampagnes waarover ik het zojuist had. Het is dus en-en. Maar iedereen die veel bezig is met het onderwerp cyber, zal weten dat de weerbaarheid echt ook bij onszelf begint. Dat wilde ik dus nog wel benadrukken.

De heer **Eerdmans** (JA21):
Weet de minister op dit moment eigenlijk hoeveel zonnepaneelinstallaties er gehackt zijn?

Minister **Yeşilgöz-Zegerius**:
Dat zal echt voor EZK zijn, sorry. Die cijfers heb ik nu zelf niet paraat.

De heer **Eerdmans** (JA21):
Kunt u me die laten weten via de minister, uw collega?

Minister **Yeşilgöz-Zegerius**:
Ik kan die vraag doorgeleiden.

De heer **Eerdmans** (JA21):
Datzelfde geldt eigenlijk voor andere apparatuur. Daar zoomt dit rapport natuurlijk minder op in, want dit gaat met name over de zonnepanelen. Is er een omvang bekend van de schade die wij nu al hebben als gevolg van de zeer magere veiligheidsnormen die worden gehaald? Uit het rapport blijken extreem slechte resultaten. Ik vind het eigenlijk onaanvaardbaar, zou ik zeggen als ik minister was, dat het op die manier eigenlijk zo lek is als een mandje, terwijl de eisen nu al vrij stevig zijn. Hoe kijkt de minister daarnaar?

Minister **Yeşilgöz-Zegerius**:
Voor een heel end was ik het heel erg eens met de heer Eerdmans, maar om daar nou meteen aan toe te voegen dat alles zo lek is als een mandje, doet hoe wij het in ons land hebben opgetuigd wel tekort, denk ik. Maar deze vragen zijn echt specifiek voor de minister van Economische Zaken en Klimaat. Als ik mij niet vergis, is er vanmiddag ook een debat over de Telecomraad, meen ik, om 16.30 uur. Ik zal de vragen dus sowieso doorgeleiden. Als het lukt om het antwoord met de cijfers daar al te geven, dan zal dat ongetwijfeld gebeuren, en anders gebeurt het schriftelijk.

De heer **Eerdmans** (JA21):
Dank daarvoor. Maar als ik constateer dat het rapport schrijft dat geen enkele, geen enkele van de onderzochte apparaten voldeed aan de veiligheidseisen, dan noem ik dat "zo lek als een mandje" met gevoel voor understatement. Kan de minister dan nogmaals duiden waarom dat een verkeerde duiding daarvan is?

Minister **Yeşilgöz-Zegerius**:
Ik geef daarbij aan dat we alles op alles zetten om er in ieder geval voor te zorgen dat we zo weerbaar mogelijk zijn. Dat betekent: aan de kant van de gebruiker. Dat betekent: aan de kant van de fabrikanten. Ik benadruk daarbij dat we zeker niet gaan zitten wachten op nieuwe wetgeving, dat er ook nieuwe wetgeving onderweg is en dat die weerbaarheid natuurlijk op heel veel verschillende manieren zeker wordt geboden. Dat was de nuance die ik daar graag in wilde aanbrengen, maar ik zal zowel de zorgen als de concrete vragen over de aantallen zeker doorgeleiden naar Economische Zaken.

De heer **Eerdmans** (JA21):
Ik ben hier overigens niet degene die de boel probeert op te pompen, want de inspectie zegt zelf dat het eigenlijk niet de vraag is of het gebeurt, maar wanneer het gebeurt. Dan heeft ze het over de digitale hack, de superhack, de cyberhack. Dat zegt de rijksinspectie zelf. De vraag is dus of u niet iets te argeloos bent in dit opzicht, dus met betrekking tot de gevaren die we misschien nog niet zien — we zien de cijfers graag tegemoet — maar vooral die ons mogelijk te wachten staan. Dan hebben we het over de kleine schade, maar zeker ook over de totale schade die aan heel veel vormen van onze digitale infra kan worden aangericht.

Minister **Yeşilgöz-Zegerius**:
Integendeel. Ik gaf aan dat het transport, de distributie en de productie van elektriciteit door EZK als vitale processen zijn aangemerkt. Daar hoort bij dat vervolgens de rijksinspectie daarop monitort en analyseert. De zaken die geconstateerd worden, worden vervolgens gedeeld. En daarnaar handelen we. Het is dus juist niet vanuit een houding van "het zal wel loslopen". Het tegenovergestelde is het geval. We zitten er juist bovenop door al deze stappen in te bouwen. Op het moment dat er een advies of een analyse ligt, gaan wij er meteen mee aan de slag. Een flink deel van deze analyse zal bij EZK uitkomen; vandaar dat ik ook verwijs naar de minister. En wat de onderdelen die bij mij liggen betreft zitten we er bovenop.

De **voorzitter**:
Dank, meneer Eerdmans. Er is een aantal vervolgvragen. Graag kort. Allereerst mevrouw Leijten, SP.

Mevrouw **Leijten** (SP):
Als alle andere onderzochte partijen niet voldoen aan de normen die zijn gesteld, dan is dat echt zorgwekkend. Maar de houding van de overheid is ook zorgwekkend. Iedereen die een zonnepaneel neemt omdat hij het goede wil doen voor het klimaat, krijgt automatisch een slimme meter. Pas als je zegt dat je dat niet wilt, krijg je een digitale meter. Daar moet je dan dus heel bewust van afzien, terwijl op die

slimme meter kan worden ingebroken. Die meter kan die omvormer, die je nodig hebt voor het energiesysteem, laten opblazen en vormt dus een risico. Zou het nou niet beter zijn, vraag ik de minister van Justitie, als we zeggen: je doet in principe niet automatisch, maar alleen als je het zelf wil mee met een slimme meter? Dan heb je veel minder toegang tot het net, wat daardoor veel minder hackbaar is.

Minister **Yeşilgöz-Zegerius**:
Ik wil niet in herhaling vallen, maar een groot deel van de vragen betreft EZK. Overigens begrijp ik wel dat deze vraag aan mij gesteld wordt. Het gaat namelijk ook over onze algehele weerbaarheid. Dit is één voorbeeld, maar alles wordt gedigitaliseerd en alles wordt slimmer en efficiënter. Op zich zijn we er heel blij mee, maar vervolgens lopen we op onderdelen gevaar. Ik denk dat we elkaar sowieso vinden in de alertheid dat je aan de voorkant de risico's moet kennen. We komen een heel eind bij elkaar. Een slimme meter heeft heel veel voordelen, maar je kunt nog nadrukkelijker aangeven wat de potentiële nadelen ervan zijn en hoe je jezelf daartegen kunt beschermen. De overheid moet dan nog steeds al die stappen zetten waar ik het over had — wij moeten ook alles op alles zetten — maar mensen weerbaar maken hoort daar wel bij. Ik zal dit zeker ook meegeven richting EZK.

Er is een paradox als je iets als zeer urgent gaat aanwijzen en daarna zegt dat er een toezichthouder komt die controleert en daarover communiceert, waarna wij handelen. Ik ben blij dat nu in ieder geval op tafel ligt waar het aan ligt. Dat is ook precies het doel geweest van het onderzoek van de rijksinspectie. Zo hebben we het ook met elkaar besproken. Nu is het handelen. In de nieuwe Nederlandse Cybersecuritystrategie is dit een cruciale lijn, maar dat is ook weer een ander debat. Het gaat erom mensen weerbaar te maken en ervoor te zorgen dat de apparatuur die we in huis halen, veilig is.

De heer **Van Haga** (Groep Van Haga):
Het is mooi dat de minister het heeft over het weerbaar maken van mensen, want het gaat natuurlijk ook een beetje om de eigen verantwoordelijkheid. Ik vraag mij af of wij onszelf niet veel te bang aan het maken zijn. Wij hebben volgens mij 20 miljoen installaties en, ik schat, 60 miljoen omvormers. Die staan bijna allemaal op huizen. Als de Chinezen mijn omvormer willen uitzetten, be my guest. Als ze mijn vaatwasser willen hacken, be my guest. Er zijn 600 professionele grote installaties in Nederland. Ik neem aan dat die goed beveiligd zijn. Mijn vraag is: zijn we onszelf niet veel te bang aan het maken? Is het niet zo dat we die professionele organisaties gewoon goed beveiligd hebben? Die zijn professioneel aangelegd. En op die huizen, ja, is het allemaal prima. Je moet gewoon je wachtwoord wijzigen en dan is het goed.

De **voorzitter**:
Uw vraag is helder.

De heer **Van Haga** (Groep Van Haga):
Ik zie het grote gevaar vanuit China gewoon niet om al die 60 miljoen omvormers te hacken.

Minister **Yeşilgöz-Zegerius**:
Ons hele leven is al naar digitaal verhuisd of beweegt in die richting. Dat geldt in ieder geval voor veel mensen. Dat brengt ook heel veel voordelen met zich mee. Het is altijd goed om alert te zijn en ook zelf in de gaten te houden hoe je jezelf het beste kunt beveiligen. Als het gaat om een slim apparaat in je huis, kan ik heel erg meevoelen met de heer Van Haga als hij zegt: waarom zou iemand mijn vaatwasser willen hacken? Maar je moet wel weten hoe je jezelf kunt beschermen. Als het een password heeft, moet je dat goed instellen en regelmatig vervangen. Dat creëert een bewustwording voor al die andere onderdelen waar we in andere debatten ook vaak bij stilstaan. We weten dat cybercrime — dat is weliswaar iets anders, maar het is ook van invloed — de snelst stijgende vorm van criminaliteit is. Heel veel Nederlanders worden daar slachtoffer van. We moeten dus continu leren om te weten hoe we onszelf zo weerbaar mogelijk kunnen maken. Daar is, denk ik, niks op tegen, juist niet. Aan de andere kant moeten we er vooral voor zorgen dat we onze vitale sectoren aan de voorkant goed beveiligen. Verder moeten we mensen ook geen angst aanjagen. Maar daartussen valt nog wel een wereld te winnen, denk ik.

Mevrouw **Rajkowski** (VVD):
Als het inderdaad misgaat, is het zeker een kwestie van nationale veiligheid. Het kan niet alleen een persoonlijk drama zijn, maar apparaten kunnen ook toegang geven tot grotere netwerken en kunnen ook gebruikt worden door kwaadwillenden. Wat de VVD betreft is het dus zeker een kwestie van nationale veiligheid. Het kabinet is op ons verzoek al bezig met de vitale sectoren te scannen en de aanbesteding vanuit de rijksoverheid aan te passen, maar waar ik naar op zoek ben, is: kunnen wij niet ook de aanbestedingen voor de vitale infrastructuur aanscherpen? Dat betekent dat we ook daar kijken naar het weren van producten en diensten uit landen met een offensief cyberprogramma, dat installateurs geen onveilige producten mogen afleveren en dat landen die onveilige cybersecurityproducten leveren ook aan minimumeisen moeten voldoen.

De **voorzitter**:
Ik wil aan de leden het volgende vragen. Een vraag is echt maximaal 30 seconden.

Minister **Yeşilgöz-Zegerius**:
We gaan nu van de vaatwasser naar een iets grotere, maar ook belangrijke scope. Ik weet dat de Kamer deze debatten en gesprekken al langere tijd voert, met mij maar ook met mijn collega's. Waar het op neerkomt, is dat wij nou eenmaal afhankelijk zijn van andere landen, ook van landen waar we misschien, als we vanaf nul zouden kunnen beginnen, alle resources hadden en net zo groot waren als die landen, helemaal niet afhankelijk van zouden willen zijn. Maar dat is niet het geval. We zijn afhankelijk. Daarbinnen moet je vervolgens kijken: wat zijn dan de vitale sectoren, wat zijn zeer gevoelige instrumenten, wat wil je extra beveiligen en waar zit dan de controle op? We hebben met elkaar afgesproken dat je vervolgens daarop focust. In die stappen zijn we. Dat betekent dat er voor vitale aanbieders al mogelijkheden zijn om eisen te stellen. Dat wordt al gedaan en we leren ook steeds meer, dus dat wordt steeds meer aangescherpt. Voor die onderdelen waar mevrouw

Rajkowski het terecht over heeft en waarvan zij zegt "misschien is het niet voor alles en iedereen altijd een probleem, maar als je inzoomt op wat je als land echt wil beschermen, dan is het wel een probleem", kunnen die eisen al gesteld worden. Volgens mij hebben we nog voor de zomer samen een debat om daar specifiek op in te gaan, en anders kom ik haar sowieso nog tegen.

Mevrouw **Dekker-Abdulaziz** (D66):
Het stemt mij optimistisch dat we het vandaag twee keer over de Cyber Resilience Act mogen hebben, waarvoor ik eerder rapporteur was. Deze wetgeving stelt hogere eisen aan slimme apparaten. Helaas gelden die eisen alleen op het moment dat de wet aangenomen is en deze producten op de markt komen. Wat gaat de minister doen om ervoor te zorgen dat ook bestaande slimme apparaten voldoen aan de veiligheidseisen van de Cyber Resilience Act?

Minister **Yeşilgöz-Zegerius**:
Ik denk dat die vraag vanmiddag echt voor EZK is. Ik ben natuurlijk de coördinerend bewindspersoon op dit onderdeel. Zoals we aanvankelijk ook met elkaar hebben afgesproken, is elke vakminister vervolgens verantwoordelijk voor de eigen coördinerende rol. Je zult dus aan de ene kant zien — mijn collega van EZK zal dat ook vertellen — dat er bijvoorbeeld een nieuwe Energiewet komt waar precies de afbakening in zit waar de VVD het over had, en dat we ondertussen fabrikanten aanspreken en mensen weerbaar maken in afwachting van de wet. Dat is wat zij zal toelichten. Wellicht kan ze ook nog concreet ingaan op precies die onderdelen die ze voor komend jaar aan het inrichten is.

De **voorzitter**:
Dan wil ik de minister van Justitie en Veiligheid danken voor haar aanwezigheid hier.