11
Digitalisering infrastructuur

Aan de orde is het **dertigledendebat** over **digitalisering van de infrastructuur**.

De **voorzitter**:
Aan de orde is het dertigledendebat over digitalisering van de infrastructuur. We hebben drie sprekers van de zijde van de Kamer en de eerste is de heer Van der Lee van de fractie van GroenLinks. Hij heeft zoals iedereen drie minuten spreektijd. Het woord is aan hem.

De heer **Van der Lee** (GroenLinks):
Dank u wel, voorzitter. Digitalisering is een zegen. Door slimme toepassingen zijn er nog gigantische mogelijkheden om energie te sparen, auto's te delen of ons beter te beschermen tegen het water. KPN becijferde onlangs dat door slimme digitale toepassingen tot 73 miljoen ton aan CO_2 te besparen valt. Onbetwist is ook de economische potentie van digitalisering en wie weet transformeert Nederland nog wel in een heuse Dutch digital valley.

Maar digitalisering kan naast een zegen ook een vloek zijn. Afgelopen maandag beweerde Willem Buiter, de hoofdeconoom van de Citigroup, nog dat 80% van de oorzaken achter toegenomen ongelijkheid tussen arm en rijk en de stagnatie van lonen in de middenklasse verklaard kan worden uit technologische ontwikkelingen. Dit risico op tweedeling is een van de publieke waarden die volgens het Planbureau voor de Leefomgeving in het geding is in dit digitale tijdperk.

In zijn signaleringsrapport gaat het PBL in op andere publieke waarden als privacy en transparantie maar heel nadrukkelijk ook op de veiligheid van onze infrastructuur. Terecht wordt geconstateerd dat digitalisering als infrastructuur der infrastructuren in toenemende mate de benutting van en de dienstverlening van al onze netten bepaalt. Of het nu gaat om de luchtvaart, wegen, spoor, water of het elektriciteitsnet, overal waar digitalisering sturend wordt in onze infrastructuur, neemt de kwetsbaarheid toe.

Nu draagt de minister van Economische Zaken niet de verantwoordelijkheid voor alle infra in ons land, maar we weten ook dat vooral het energienet het meest geliefde doelwit is van hackers. Het PBL rapporteert over zes verschillende wijzen waarop digitalisering de leveringszekerheid bedreigt en ook werd recent bekend dat het aantal ransomwarevarianten afgelopen jaar met maar liefst 122% is gegroeid.

Economische schade is te gemakkelijk op grote schaal toe te brengen, zoals we onlangs nog zagen in de Rotterdamse haven. Onze cybersecurity is nog lang niet op orde, ook al worden er nieuwe stappen gezet, zoals het Digital Trust Center voor het mkb. Daarom heb ik toch het verzoek aan de minister van Economische Zaken om nader in te gaan op de zeven handvatten die het PBL aanreikt om te voorkomen dat digitalisering beschermende waarden ondermijnt. Ik hoop dat u, minister, op al die zeven punten in kunt gaan. Ik ga ze hier niet herhalen.

Maar er is ook dringend behoefte aan versterking van de capaciteit en het sturingsvermogen van de overheid. Vindt u, minister, ook dat een sterke investering op dit terrein gerechtvaardigd is? Nu weet ik dat de minister het niet is gelukt om de reactie op dit rapport af te stemmen met andere bewindslieden, want digitalisering als onderwerp is nogal verspreid. Ik zou een dringend beroep op hem willen doen om in zijn laatste dagen als minister toch zijn wijze lessen te delen over hoe de overheid om moet gaan met de spanning tussen digitalisering en publieke waarden.

Op één punt hoop ik dat hij, of anders de collega's per motie, vandaag nog een stap verder wil gaan. De kansen en risico's van de onvermijdelijk voortschrijdende digitalisering zijn dermate groot dat die de portefeuille van één bewindspersoon overstijgen. Een alliantie van 30 bedrijven, maatschappelijke organisaties en kennisinstellingen heeft onlangs gepleit voor het instellen van een aparte digitale onderraad. Bent u met mij van mening dat zo'n extra onderraad van de ministerraad een integrale aanpak van de digitale dilemma's kan borgen?

Dank u wel.

De **voorzitter**:
Dank u wel. Dan de heer Hijink van de fractie van de Socialistische Partij.

De heer **Hijink** (SP):
Voorzitter. Het publieke belang sneeuwt een beetje onder. Ik vond het een mooi understatement van mevrouw Snellen, onderzoeker bij het Planbureau voor de Leefomgeving. Je kunt het ook steviger stellen: het is mogelijk voor slimme hackers om onze stroom af te sluiten, om onze fabrieken stil te zetten en om het licht in huizen uit te schakelen. Dat is goed voor een nieuwe geboortegolf, maar ook een groot gevaar voor onze economie, de volksgezondheid en onze veiligheid.

Begin vorige maand werd bekend dat het hackerscollectief Dragonfly 2.0 in staat is om tientallen energiebedrijven in de Verenigde Staten en Europa over te nemen, letterlijk tot het niveau waarop elektriciteit in huishoudens en bedrijven kan worden afgesloten. Kan de minister aangeven of Nederlandse energieleveranciers door deze aanval geraakt zijn? Welke andere landen in Europa zijn getroffen en in hoeverre komt onze elektriciteitsvoorziening in gevaar als onze buurlanden te maken krijgen met grootschalige blackouts? We weten dankzij het werk van Willem Westerhof, een onderzoeker en ethisch hacker, ook dat de omvormers voor zonnepanelen eenvoudig te hacken zijn. Het uitschakelen van duizenden systemen is dan mogelijk, met massale uitval van elektriciteit tot gevolg. Hoe reageert de minister op deze kwetsbaarheid in onze elektriciteitsvoorziening?

In juni steunde de Tweede Kamer het voorstel dat ik samen met de heer Verhoeven van D66 deed om meer maatregelen te nemen om apparatuur die verbonden is met het internet beter te beveiligen. Gaat de minister deze aangenomen motie nog uitvoeren? Waarom wordt er gewacht op maatregelen uit Brussel voordat wij zelf aan de slag gaan? Is de minister bereid om te onderzoeken hoe we in een samenwerkingsverband tussen de overheid, het bedrijfsleven,

hackers en cybersecurityexperts deze apparaten met hacktests kunnen testen?

Voorzitter. Wat de SP betreft moet de overheid de veiligheid, de leveringszekerheid en de gelijke toegang van onze infrastructuur beschermen. De vraag is of dat op dit moment wel voldoende gebeurt. Is ons land voorbereid op grootschalige aanvallen op onze stroomvoorziening? Hebben we in beeld hoeveel onveilige omvormers in Nederlandse huizen hangen? Heeft de overheid voldoende kennis in huis om de permanente strijd tussen hackers en beveiligers te kunnen winnen? De vraag die het Planbureau voor de Leefomgeving terecht stelt is welke publieke waarden wij in ons land willen beschermen.

Als de overheid de hoeder is van het collectieve belang, past het niet om de verantwoordelijkheid voor de veiligheid en zekerheid af te schuiven op de mensen die moeten kunnen rekenen op veilige apparatuur. Dan moet je als overheid zelf het voortouw nemen en voorop blijven lopen, niet wegkijken als elektriciteitsbedrijven gehackt kunnen worden en optreden als Nederlandse huishoudens worden volgestopt met onveilige apparatuur. Ik hoor heel graag van de minister of hij het voorstel van de SP om vaker apparatuur te testen op de beveiliging ervan vanavond of later wil ondersteunen.

De **voorzitter**:
Dank u wel. Dan de heer Jetten van de fractie van D66.

De heer **Jetten** (D66):
Dank u wel, voorzitter. Als het gaat over cyber, verwacht u natuurlijk allemaal mijn collega Verhoeven hier achter het katheder, maar vanavond mag u het met mij doen. Dat is maar goed ook, want digitalisering is een van de grote krachten van verandering in onze samenleving, en het is goed dat we daar in deze Kamer over praten en dat het breder wordt dan alleen die paar Kamerleden wie cyber al een aantal jaren na aan het hart ligt. Mensen, bedrijven en overheden gebruiken steeds meer digitale technologie, en we hebben het er in deze Kamer te weinig over.

Aanleiding voor het debat van vandaag is een uitstekend rapport van het Planbureau voor de Leefomgeving over mobiliteit en elektriciteit in het digitale tijdperk. Digitalisering biedt kansen maar brengt ook uitdagingen met zich mee. Digitalisering kan publieke waarden als toegankelijkheid, veiligheid en privacy onder druk zetten. Dat vereist politieke aandacht en sturing. Collega Van der Lee verwees zonet al naar het voorstel voor een digitale onderraad die zich daar specifiek mee bezighoudt. Ik ben erg blij dat een aantal organisaties en nu ook GroenLinks dit voorstel van collega Verhoeven van D66 omarmen.

Laat ik een voorbeeld pakken dat dichter bij mijn eigen portefeuille ligt, namelijk infrastructuur en mobiliteit: zelfrijdende auto's. Dat biedt kansen. We zien allemaal de mooie plaatjes voor ons. Over tien, vijftien jaar kunnen we in een auto de krant lezen. Er gebeuren minder verkeersongelukken, er zijn minder files, en daarmee is de zelfrijdende auto ook beter voor de economie. Maar zelfrijdende auto's brengen ook uitdagingen met zich mee. Hoe gaan we om met de data die deze auto's genereren? Hoe zorgen we ervoor dat die auto's niet worden gehackt? Hoe gaan we om met de algoritmes die complexe keuzes moeten maken over de verkeersveiligheid? Ziet de minister deze uitdagingen ook?

Voorzitter. Niet alle digitalisering is noodzakelijk. Soms willen we dingen digitaliseren die we misschien beter niet moeten digitaliseren, zoals het stemproces of bepaalde onderdelen van onze vitale infrastructuur die we willen beschermen tegen hacks. Is de minister dit met mij eens? Hoe vindt die afweging plaats als het gaat om de digitalisering van onze vitale infrastructuur?

Voorzitter. Het PBL heeft een goed rapport afgeleverd, dat goede handvatten geeft om de komende jaren de discussie over digitalisering te voeren. Het werpt ook nieuwe dilemma's op, en we moeten goed nadenken over de gevolgen van beleid en wetten voor onze publieke waarden, over cybersecurity en over privacy. Deelt de minister deze conclusies van het PBL?

Het PBL wijst ook terecht op de noodzaak van digitale kennis, niet alleen bij mensen en bedrijven, maar ook bij de overheid en de Kamer. Daar hebben we ook af en toe hulp van buiten voor nodig. Daarom tot slot nog twee concrete vragen. Vorige week liet de gemeente Den Haag hackers de IT-systemen testen, een zogeheten bug bounty challenge. Eerder liet bijvoorbeeld ook de brandweer zijn brandweerwagens testen. Is de minister bereid om dit soort challenges ook op rijksniveau te organiseren?

Mijn tweede vraag gaat over het gebruik van algoritmes door de overheid. Algoritmes zijn niet per definitie neutraal en kunnen grote gevolgen hebben voor mensen. Bestaat er overzicht van overheidsdiensten, zowel op niveau van het Rijk als op niveau van gemeenten, waar algoritmes gebruikt worden om beslissingen te nemen? Zo nee, is de minister bereid om zo'n overzicht te maken?

Dank u wel.

De **voorzitter**:
Een vraag van de heer Bosman.

De heer **Bosman** (VVD):
Ik hoor de heer Jetten even tussendoor zeggen dat er processen zijn die je niet zou moeten willen digitaliseren. Dat vind ik heel bijzonder, want er wordt alleen iets genoemd over het stemproces, bijvoorbeeld. Is dat het enige, of zegt u: nou, er zijn wel meer processen die we niet zouden moeten digitaliseren? Of zouden we een infrastructuur moeten maken waarbij je wél zou kunnen stemmen met digitalisering?

De heer **Jetten** (D66):
De discussie over het stemproces wordt hier vaak genoeg gevoerd, denk ik. De commissie Infrastructuur en Milieu had laatst een gesprek met de Deltacommissaris. Er liggen grote opgaven voor vernieuwing van onze waterwerken en ook voor de bescherming daarvan. Daar moet je dus continu de afweging maken: kan digitalisering de waterveiligheid versterken of zijn we onvoldoende in staat om de digitalisering van die waterwerken nu zo goed te beveiligen dat we zeker weten dat ze niet gehackt kunnen worden? Je moet daar continu kijken wat digitalisering toevoegt. Soms moet

je dan beslissen om juist op oude systemen en technieken te blijven vertrouwen, omdat die op dit moment veiliger zijn.

De heer **Bosman** (VVD):
Dat vind ik heel bijzonder, want dat zou ook iets kunnen betekenen voor bijvoorbeeld de luchtvaart. Misschien moeten we de luchtvaart dan maar niet digitaliseren. Of de auto's. U — sorry: de heer Jetten — was heel enthousiast over zelfrijdende auto's. Maar dat kan heel gevaarlijk worden. Als die te hacken zijn, is dat een probleem. Ik ben nu toch een beetje in de war over wat D66 precies wil.

De heer **Jetten** (D66):
Laat ik de heer Bosman daar dan bij helpen. Hij kiest nu zelf het voorbeeld van de luchtvaart. Daar is al sprake van een grote mate van digitalisering. Maar als je kijkt naar de systemen van bijvoorbeeld de luchtverkeersleiding, dan zijn dat oude systemen, die steeds meer onder druk staan, niet alleen omdat ze de capaciteit van het huidige vliegverkeer niet aankunnen, maar ook omdat hackers steeds beter in staat zijn om die systemen aan te tasten. Dus waar er sprake is van digitalisering, moet je continu proberen om die verder te versterken en te verbeteren. Waar er nog geen sprake is van digitalisering, zijn er natuurlijk altijd kansen, maar ik denk dat dit rapport ook goede aanleiding geeft om dan niet als een paard zonder kop achter die kansen aan te rennen, maar continu te blijven nadenken of digitalisering nu een goede stap voorwaarts is of dat we eerst verder moeten verbeteren en versterken voordat we die kant op gaan.

De **voorzitter**:
Afrondend. Kort. O, ik zie dat u al klaar bent. Heel goed. Dan mevrouw Bruins Slot.

Mevrouw **Bruins Slot** (CDA):
Ik heb nog een korte vraag op een ander punt. Het is heel goed dat de heer Jetten ook ingaat op het gebruik van algoritmes, want dat is niet waardevrij. Er worden natuurlijk bepaalde beslispatronen in opgenomen die gewoon keuzes inhouden. Hoe wil de heer Jetten daar meer zicht op krijgen? We hebben natuurlijk privacy-impactassessments als het gaat om gegevensbescherming. Maar hoe zou je dat met algoritmes kunnen doen die de overheid ook gebruikt om bepaalde beslispatronen in kaart te brengen?

De heer **Jetten** (D66):
Mijn vraag nu aan de minister is om in ieder geval in kaart te brengen waar we de algoritmes al toepassen, zodat we dat beter kunnen volgen en kunnen analyseren in hoeverre we dat op een goede manier doen. Ik ben jarenlang gemeenteraadslid geweest en dan zie je dat op lokaal niveau algoritmes steeds meer worden gebruikt om bijvoorbeeld fraudes op te sporen of beslissingen te nemen op het gebied van zorg of werk. We moeten uitkijken dat we niet onbewust discriminerende aspecten toevoegen aan zo'n algoritme. Het lijkt me dus goed om in kaart te brengen welke algoritmes er zijn, zodat we ook beter in staat zijn om het te blijven controleren. Mocht het dan de verkeerde kant op gaan, kunnen we tijdig ingrijpen.

De **voorzitter**:
Dank u wel. We gaan luisteren naar de bijdrage van mevrouw Bruins Slot. Het woord is aan haar.

Mevrouw **Bruins Slot** (CDA):
Voorzitter. Het CDA vindt dat het Planbureau voor de Leefomgeving een goed rapport heeft geschreven over de voortsnellende digitalisering van infrastructuur en publieke waarden. Het CDA deelt ook de opvatting van het Planbureau voor de Leefomgeving dat ICT-innovaties een enorme impuls geven aan de doelmatige en duurzame benutting van infrastructuur en dat dat enorme meerwaarde heeft. Het bedrijfsleven speelt hierbij natuurlijk ook een belangrijke rol.

Maar het planbureau benadrukte ook zeer nadrukkelijk dat er een keerzijde is. De heer Van der Lee ging daar ook al op in. Het PBL waarschuwt voor een tweedeling in de samenleving van hoger en lager opgeleiden, van ouderen en bijvoorbeeld mensen met een licht verstandelijke beperking. Maar er zijn ook nog steeds gebieden in Nederland, de heer Kamp weet dat, die geen breedbandinternet hebben. Het CDA herkent dit gevaar van tweedeling. De overheid heeft hier een taak. Hoe kijkt de minister aan tegen dit spanningsveld?

Voorzitter. Een tweede keerzijde is de kwetsbaarheid van digitale infrastructuur. De SP en GroenLinks hebben daar ook al een aantal vragen over gesteld. Doordat we steeds afhankelijker worden van ICT, kunnen de gevolgen van de activiteiten van hackers, maar bijvoorbeeld ook van statelijke actoren — lees de rapporten van de Algemene Inlichtingen- en Veiligheidsdienst — steeds groter worden. Het platleggen van de elektriciteitsvoorziening kan drastische gevolgen hebben. De vraag aan de minister, die overeenkomt met de vragen van de SP en GroenLinks, is hoe we ervoor zorgen dat de veiligheid van bijvoorbeeld onze elektriciteitsvoorziening gelijke voet houdt met de digitalisering.

Voorzitter. Het rapport stipt ook juridische en ethische dilemma's aan. Laten we inderdaad die zelfrijdende auto van de heer Jetten nemen. Een zelfrijdende auto bestaat inmiddels gewoon. Die moet afwegingen maken op het moment dat hij op het punt staat om tegen iemand aan te botsen: wie ga ik beschermen, degenen die in de auto zitten of degenen die ik aanrij? Dat is iets wat ook in de software van de auto geschreven staat. Daarbij wordt een ethische afweging gemaakt, want waar laat je de schade het grootst zijn? Het kan dus ook gaan om zelflerende software die een fout maakt met schade tot gevolg. Hoe bereidt de regering zich voor op dergelijke dilemma's, dus op de dilemma's van de zelfrijdende auto, maar ook het dilemma van zelflerende software die een fout maakt?

Eigenlijk komt het Planbureau voor de Leefomgeving tot dezelfde conclusie als het rapport van het Rathenau Instituut met de titel Opwaarderen. Het gaat erom dat we de publieke waarden van veiligheid, privacy, toegankelijkheid, beschikbaarheid en leefbaarheid van voorzieningen ook toepassen in de digitale omgeving. We hoeven dus geen nieuwe waarden te maken, maar moeten er vooral voor zorgen dat we de oude waarden voor het digitale tijdperk geschikt maken. Dat kan bijvoorbeeld door het techniekon-

afhankelijk maken van onze huidige publieke waarden, maar ook bijvoorbeeld het techniekonafhankelijk maken van wetgeving. Kan de minister een update geven van de vorderingen die op dit terrein worden gemaakt?

Dank u wel, voorzitter.

De **voorzitter**:
U bedankt. Dan de laatste spreker van de zijde van de Kamer, de heer Bosman van de fractie van de VVD.

De heer **Bosman** (VVD):
Voorzitter. Het is heerlijk om vanuit je bed op de smartphone het nieuws te bekijken, dan een warme douche te nemen en dan vervolgens met de trein naar het werk te gaan, alledaagse dingen die zonder een betrouwbaar energiesysteem niet mogelijk zijn.

De digitalisering van de energiesector brengt ons naast vele voordelen ook nieuwe risico's. Cyberaanvallen op ons energiesysteem kunnen zorgen voor een grote impact op de samenleving. Netbeheerders en energieleveranciers moeten samen optreden om te voorkomen dat ons systeem succesvol wordt aangevallen. Welke mogelijkheden hebben bedrijven hiervoor? In hoeverre is er bij het toetsen van de weerbaarheid van die systemen een rol weggelegd voor het Nationaal Cyber Security Centrum? Hoe kan de sector samen met de overheid werken aan een betrouwbare energievoorziening?

Een betrouwbare, betaalbare en schone energievoorziening is makkelijker gezegd dan gedaan. Deze minister heeft samen met de energiesector een stap gezet naar de toekomst, een transitie waarin naast de verduurzaming van de energie ook de betrouwbaarheid en de betaalbaarheid niet uit het oog verloren zijn.

Dank u wel, voorzitter.

De **voorzitter**:
U bedankt. Dat was de termijn van de Kamer. De minister is in staat om meteen te antwoorden. Het woord is aan hem.

Minister **Kamp**:
Voorzitter. Terecht zeiden eigenlijk alle woordvoerders dat zich door de digitalisering grote kansen voordoen voor ons als samenleving. Ik ga daar zo wat nader op in, en ook op de dingen die daaraan verbonden zijn. Enkele woordvoerders zeiden ook dat er grote risico's aan verbonden zijn, bijvoorbeeld voor onze energievoorziening. Mevrouw Bruins Slot zei ook dat we ook te maken kunnen krijgen met andere landen die bedreigingen voor ons kunnen vormen door iets te doen met de digitalisering die wij in ons land hebben doorgevoerd. Wat mevrouw Bruins Slot zegt, is absoluut waar. Ik kan mij voorstellen dat als er tegenwoordig weer een groot conflict ontstaat, een land dat zo'n conflict aangaat de mogelijkheid heeft om de verkeersleiding in een ander land plat te leggen, de energievoorziening plat te leggen of het verkeer in de war te gooien. Er zijn allerlei dingen in een land die gedigitaliseerd zijn. Als je dat in de war schopt, veroorzaak je chaos in zo'n land. Ik kan mij heel goed voorstellen dat dat de opmaat zou kunnen zijn tot een conflict. Ook in de verhouding tussen staten is het heel relevant om je te realiseren welke risico's je loopt. Andere woordvoerders zeiden ook dat hackers in systemen kunnen binnendringen en daar beschadigingen kunnen aanbrengen. Dat kan allemaal.

Vorig jaar waren er in de energiesector een heleboel storingen, enkele tienduizenden. In totaal traden er zo'n 20.000 storingen op de een of andere manier op, waarvan er ruim 19.000 tot een onderbreking van de energievoorziening op kleine of soms op iets grotere schaal hebben geleid. We kunnen elkaar op dit moment nog even gelukwensen dat geen een van die onderbrekingen is veroorzaakt door een probleem met de digitalisering. Het probleem doet zich nog niet voor, maar dat wil absoluut niet zeggen dat het zich niet gaat voordoen en dat we het niet heel serieus moeten nemen. Wij nemen het als overheid bijzonder serieus. De netwerken waarmee je de energie, gas en elektriciteit, naar de afnemers moet brengen, zijn cruciaal. In 2015 hebben we in de Elektriciteitswet de beheerders van die netwerken verantwoordelijk gesteld. Op grond van artikel 16 van de Elektriciteitswet heeft een netwerkbeheerder in het kader van de beheer van de netten de taak om die netten te beschermen tegen mogelijke invloeden van buitenaf. In de memorie van toelichting hebben we gezegd dat onder andere cyberaanvallen daar ook onder vallen. Dat is de eerste wettelijke voorziening.

Dat is niet alles wat we hebben gedaan. De Wet gegevensverwerking en meldplicht cybersecurity is enkele dagen geleden, op 1 oktober in werking getreden. Die wet bevat een zorgplicht voor het geval dat er op de een of andere manier incidenten zijn met gegevensverwerking of met de bescherming van de digitale voorzieningen, met andere woorden, een probleem met de cybersecurity. Je hebt ervoor te zorgen dat dat zich niet of zo weinig mogelijk voordoet en dat als het zich toch voordoet, er onmiddellijk adequaat gereageerd kan worden. Bovendien is er een meldplicht vastgelegd. Dat is de tweede wettelijke voorziening die we hebben getroffen.

Dan de derde wettelijke voorziening. De heer Jetten zei dat we maar niet op Europa moesten blijven wachten. Dat doen we niet. Ik heb al aangegeven dat we zowel in 2015 als in 2017 wetten in werking hebben laten treden die zeer relevant zijn voor het onderwerp dat we nu bespreken. Daarnaast is er een Europese richtlijn, de zogenaamde NIB-richtlijn voor netwerk- en informatiebeveiliging. Wij zullen die begin volgend jaar implementeren in een wet. Op die manier hebben we de zaak breed op orde gebracht en brengen we die nog verder op orde in wetgeving.

Het is een heel breed onderwerp. Ik heb even gesproken over de energienetwerken en de heer Jetten sprak over de zelfrijdende auto's, ook een voorbeeld van digitalisering. Hij zei dat er daar ook ontwikkelingen zijn. Dat is zeker waar. We lopen ook daarmee absoluut risico's en dat moeten we ons heel goed realiseren. Mevrouw Bruins Slot zei al dat er op een gegeven moment beslissingen moeten worden genomen. Zo'n zelfrijdende auto neemt die beslissingen, maar dat wordt via de software ingebracht. Als overheid moet je je daarvan bewust zijn en moet je vanuit ethische overwegingen ook daarbij betrokken willen zijn. Daar kom ik straks nog wat verder over te spreken.

Er zijn ook heel praktische dingen aan de orde. Op een gegeven moment is er bijvoorbeeld een blinde die oversteekt met een rode stok. Het verschil tussen iemand die gewoon oversteekt en iemand die met rode stok oversteekt, zie je als bestuurder en dan weet je wat je moet doen. Maar kan ook zo'n zelfrijdende auto dat, is dan de vraag. Op een gegeven moment wordt er iets verkeerd gedaan. Als nu een bestuurder iets verkeerd doet op de weg, kun je die een bekeuring geven. Maar stel nou dat er iets verkeerd wordt gedaan door zo'n zelfrijdende auto. Wie is daar dan verantwoordelijk voor? Degene die de software gemaakt heeft, degene die die auto verkocht heeft of degene die in die auto rijdt? Er zijn allerlei vraagstukken aan de orde.

Het is niet zo, zoals de heer Jetten zei, dat we maar blind aanlopen achter zo'n ontwikkeling als die zelfrijdende auto. We onderkennen dat dat een ontwikkeling is die speelt en dat die grote voordelen kan hebben. Die kan ertoe leiden dat we veel meer capaciteit krijgen op onze infrastructuur, op onze wegen, waardoor we minder files hebben en mensen sneller naar hun bestemming kunnen komen. Het is dus iets waar we zeker positief tegenover staan. Maar we zijn ons zeer bewust van de problemen die zich daarbij ook voordoen. I en M heeft ingezet op een ontwikkeling die inhoudt dat we leren door het te doen, learning by doing. Dat betekent dat we mogelijkheden bieden aan fabrikanten om ook in de praktijk ervaring op te doen en dat is niet zo gemakkelijk. Daar moeten allerlei voorwaarden aan gekoppeld worden natuurlijk, want we kunnen het verkeer daardoor niet in gevaar brengen. Maar het is wel nodig dat we in de praktijk ervaring opdoen, dus we spreken daarover met het bedrijfsleven. We kijken of de wetgeving adequaat is dan wel of aanpassing van de wetgeving nodig is. We bespreken met het bedrijfsleven wat de risico's zijn die zich voor kunnen doen.

We laten daar ook onderzoek naar doen. Op dit moment doet de Technische Universiteit Delft bijvoorbeeld wetenschappelijk onderzoek naar wat dan heet "meaningful human control". Dat betekent dat wordt gekeken hoe je ervoor kunt zorgen dat je wat een machine kan en wat een mens kan goed samen kunt laten gaan en elkaar kunt laten versterken. Nederland is daar zeer actief in. We willen daar ook een voortrekkersrol in spelen. Dit is iets wat internationaal speelt, we zijn dus ook zeer actief in internationaal verband om hiermee verder te komen. Maar ergens maar blind achteraan hollen, is het laatste dat we zouden kunnen verantwoorden en wat ik als bewindspersoon naar de Kamer toe zou kunnen verantwoorden.

Voorzitter. Ik heb het net gehad over waar het bij mij met name om gaat, namelijk de energievoorziening. In de eerste plaats hebben we de netbeheerders die een zorgplicht hebben. Die zorgplicht is op dit moment niet opgelegd aan de energieproducerende en aan de energiedistribuerende bedrijven, maar ik kan me voorstellen dat daar bij de toenemende digitalisering ook risico's zijn die een adequate reactie vergen. Dat betekent dat wij samen met de sectoren de ontwikkeling bekijken en bezien wat er gaande is op het punt van digitalisering, wat de mogelijke risico's zijn en wat we samen kunnen doen om die risico's op te vangen. Dan zou het heel goed kunnen zijn dat een zorgplicht zoals we die hebben voor de netbeheerders ook voor andere onderdelen van het bedrijfsleven dat zorgt voor onze energievoorziening van toepassing wordt op enig moment. Maar dat zal steeds in overleg met hen gebeuren, omdat zij als meest betrokkenen daar natuurlijk het meeste mee te maken krijgen. Zij hebben er ook het meeste verstand van en hebben er belang bij dat het allemaal op een nette manier geregeld wordt.

Voorzitter. Laat ik op de verschillende punten ingaan die de woordvoerders naar voren hebben gebracht en beginnen met de heer Van der Lee. Hij sprak over het rapport van het Planbureau voor de Leefomgeving. Hij sprak daar zijn waardering voor uit. Anderen hebben dat ook gedaan. Ik denk dat dat terecht is. Het is heel goed dat het Planbureau voor de Leefomgeving een onderwerp als dit oppakt. De handvatten waar ze mee gekomen zijn, zijn ook interessant, maar we moeten wel onder ogen zien — dat is onvermijdelijk — dat die op dit moment nog erg abstract zijn geformuleerd. Een handvat is erkennen dat de digitalisering nieuwe dilemma's opwerpt. Ja, dat erkennen we. Een ander is accepteren dat er een onontkoombare spanning is tussen de infrastructuren en de snelle virtuele werelden. Ja, dat is ook waar. Denk na over nieuwe spelregels. Ja, dat hebben wij gedaan en zullen wij blijven doen. Dus het zijn interessante handvatten — ik heb een paar voorbeelden genoemd — maar het gaat er vooral om dat wij ons bewust zijn van wat er aan de hand is, dat wij daar niet ad hoc maar op een gestructureerde manier op reageren, en dat wij dat op een zodanige manier doen dat wij daar de maximale resultaten uit halen.

Ik heb al gesproken over het energiedomein. Ik heb al een opmerking gemaakt over de netbeheerders, de energieproducenten en de energiedistributeurs. In dat verband is ook interessant dat wij al een vergaande digitalisering doorvoeren met de slimme meter. Die slimme meter wordt overal geplaatst. Dat betekent dat er dan ook andere beprijzingsmogelijkheden zijn. Nu heb je maar te betalen wat er geleverd wordt, maar straks kun je het zo organiseren dat er, afhankelijk van het aanbod, per kwartier verschillende prijzen zijn. Je kunt je gedrag van afname van gas en elektriciteit dan aanpassen. Dat betekent dat je daar weer een aparte marktwerking voor krijgt.

Dat zijn interessante mogelijkheden. Tegelijkertijd doet zich dan ook de vraagstelling voor die mevrouw Bruins Slot heeft opgeworpen. Dat is: hoe ga je om met de mensen die daar wat minder gemakkelijk mee omgaan? Hoe voorkom je een tweedeling in de samenleving door deze ontwikkeling? Ik denk dat dat een belangrijke opgave is voor de overheid. Digitalisering leidt vaak tot een betere en een laagdrempeligere toegang tot diensten en voorzieningen die voor iedereen belangrijk zijn. Het is nodig dat mensen er rekening mee houden dat de wereld verandert. Zo is dat. Daar kan niemand aan voorbij. Dat betekent dat je jezelf ook zult moeten aanpassen, maar de overheid moet dan in de gaten houden of iedereen dat wel kan, of dat er kwetsbare mensen zijn die de bescherming van de overheid nodig hebben. Een belangrijk uitgangspunt voor de overheid is dat niemand door de digitalisering de toegang tot noodzakelijke voorzieningen mag worden ontzegd. Dat betekent dat er een niet-digitaal alternatief beschikbaar moet zijn of dat het digitale middel zo ontworpen is dat het echt voor iedereen toegankelijk is, ongeacht leeftijd of opleidingsniveau.

Dat passen wij al heel concreet toe op dit moment. Ik heb het voorbeeld van de slimme meter genoemd. Wij zijn nu ook met het bedrijfsleven aan het kijken hoe je de afnameoverzichten, de prijsinformatie uit de slimme meter, zodanig aan de afnemers van de producten kunt presenteren dat

alle groepen daarmee uit de voeten kunnen. Dat is een uitdaging waar wij op dit punt al wat mee kunnen gaan oefenen.

De heer Van der Lee sprak over het voorbeeld van de afname van elektriciteit en gas en de partijen die daarbij betrokken zijn. Ik heb de wetgeving genoemd, maar van het grootste belang is ook de hele cultuur eromheen. Hoe ga je ermee om? Hoe werk je samen? Ik denk dat het heel goed is dat wij nog dit jaar een bijeenkomst gaan beleggen, waarbij wij als overheid met de sector en de toezichthouders op de sector de hele digitalisering van om te beginnen de elektriciteitsvoorziening met elkaar gaan onderzoeken. Wat speelt daar allemaal? Welke dingen doen wij op dit moment, waar zijn wij mee bezig en wat zijn wij van plan? Is dat genoeg? Hebben wij dingen vergeten? Als wij wat vergeten hebben, wat is dat en wat moeten wij daar dan aan doen?

Ik ben van plan om die bijeenkomst te beleggen en om de informatie die daaruit komt en de vervolgacties die wij met elkaar afspreken, met de Kamer te delen. Ik wil dat voor het eind van het jaar nog doen. Vervolgens ben ik ook van plan om te kijken of wij de systematiek die wij met de elektriciteitssector gebruiken, ook bij andere sectoren kunnen toepassen. Daar gaat het toch om. Het is een ontwikkeling die ingezet is en door zal gaan. Je moet zorgen dat je je als samenleving daaraan aanpast. Dat kunnen wij op deze manier doen.

De heer Van der Lee vroeg ook naar het borgen van de publieke belangen bij de digitalisering van de infrastructuur. Op één aspect daarvan heb ik net al gereageerd, in reactie op mevrouw Bruins Slot. De publieke belangen waar de heer Van der Lee op doelt, zijn belangen als toegankelijkheid, zoals ik net heb behandeld, leveringszekerheid, privacy en de democratische controle op wat we als overheid aanbieden en wat we daarvan vinden. Dat zijn de publieke belangen en die moeten ook geborgd zijn. Voor de privacy geldt de Wet bescherming persoonsgegevens. Wat betreft energie: ik heb aangegeven hoe het zit met de netbeheerders. Ik heb aangegeven dat we kijken of er voor de andere onderdelen van de energievoorziening vergelijkbare regelingen nodig zijn. Ik kan u meegegeven — dat is geen dooddoener, maar iets wat we bijzonder serieus nemen — dat de overheid, het ministerie van Economische Zaken in het bijzonder, maar ook het ministerie van Veiligheid en Justitie, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van I en M, met alle relevante sectoren voortdurend in contact blijft om met elkaar te zien wat de ontwikkelingen en de mogelijkheden zijn, wat we vinden van de verschillende aspecten die daaraan verbonden zijn en hoe we daar samen op een juiste manier mee om kunnen gaan.

De heer Hijink sprak in dit verband ook over de risico's.

De **voorzitter**:
De heer Van der Lee heeft nog een vraag.

De heer **Van der Lee** (GroenLinks):
Ik dank de bewindspersoon voor de uitgebreide beantwoording. Hij is op één aspect niet ingegaan en juist dat aspect heeft vandaag mijn speciale interesse. Hij beschreef dat verschillende partijen, met name in de energiesector, ons net, hun verantwoordelijkheid moeten nemen voor het verminderen van de kwetsbaarheid van digitalisering. Dat zie je in alle netwerken. De ontwikkeling van digitalisering als infrastructuur der infrastructuren maakt dat iedereen straks een verantwoordelijkheid heeft. Maar wie is dan eindverantwoordelijk? Dat probleem speelt zich ook af op het niveau van het kabinet zelf. Wie is op dit moment eindverantwoordelijk? In dat verband vind ik het idee om een speciale onderraad in te richten een goed antwoord, omdat dit vraagstuk in alle domeinen speelt. Je kunt niet één bewindspersoon aanwijzen als eindverantwoordelijke. Maar er is wel sprake van een collectieve verantwoordelijkheid en die moet goed geborgd zijn. Zou de minister, als misschien wel de meest ervaren bewindspersoon die nog actief is, toch zijn gedachten op dit specifieke punt van de onderraden met ons willen delen?

Minister **Kamp**:
Liever niet. Ik denk dat dat niet goed zou zijn. Ik ben, zoals mijn collega van VWS dat noemt, "diepdemissionair". In de kranten staat dat het volgende kabinet in de week van 23 oktober zou kunnen aantreden. Dit zijn mijn laatste weken als minister. Als er een nieuw kabinet is, dan gaat dat nieuwe kabinet zijn werkwijze bepalen. Dan wordt vastgesteld in welke frequentie en wanneer er wordt vergaderd, hoe de verhouding is tussen onderraden en de ministerraad, hoeveel onderraden er zijn en wie daaraan meedoen. Ik kan mij heel goed voorstellen dat het nieuwe kabinet besluit om te doen wat de heer Van der Lee bepleit; ik geloof dat de heer Jetten dat ook gedaan heeft. Dat kan ik mij goed voorstellen, maar ik zou het heel ongepast vinden als ik mij daar als bijna vertrekkende bewindspersoon mee zou gaan bemoeien. Ik heb mij heel lang met van alles en nog wat mogen bemoeien, maar straks zijn anderen aan de beurt. Ik denk dat de opvatting van de Kamer, en ook de opvatting van de heer Van der Lee, meegenomen zullen worden bij de besluitvorming daarover, omdat zijn suggestie bepaald niet onredelijk is.

De heer **Van der Lee** (GroenLinks):
Ik heb er natuurlijk begrip voor dat de minister niet op dit specifieke voorstel wil reageren vanwege zijn demissionaire status. Maar mag ik de vraag dan iets anders formuleren? Gelet op alle uitdagingen en kansen die er liggen, is er dan reden om ook op het niveau van het kabinet zelf na te denken over de vraag of de aansturing van de kansen en risico's op dit terrein op een andere en misschien iets betere manier zou moeten worden aangepakt?

Minister **Kamp**:
Ik vind de digitalisering een zeer belangrijke ontwikkeling die gaande is, met grote gevolgen, met veel kansen en ook met risico's. Ik denk dat daar meerdere bewindspersonen bij betrokken zijn. Ik zou me een coördinatieoplossing, zoals aangedragen door de heer Van der Lee, goed kunnen voorstellen.

De heer Hijink heeft een aantal opmerkingen gemaakt waar ik op in wil gaan. Wat doet de overheid tegen de risico's die het met zich meebrengt dat steeds meer apparaten met internet worden verbonden? Welke activiteiten onderneemt zij? Ten eerste: voor het verbinden van allerlei apparaten met internet geldt dat daar enorme kansen uit naar voren komen. Ik ben bij een bedrijf in de Achterhoek geweest,

waar via internet een klant een bestelling doorgeeft aan dat bedrijf. Daar komt verder helemaal geen persoon aan te pas. Dat gaat via de computer. Het bedrijf dat die bestelling binnenkrijgt, maakt bepaalde metaalproducten helemaal precies volgens specificatie van de klant. Vervolgens wordt geregeld dat die producten in een vrachtwagen komen, die dat naar de klant brengt. De enige personen die daarmee te maken krijgen, zijn degene die het product vanuit de fabriek in de vrachtwagen zet en de chauffeur die het naar de klant brengt. Voor de rest gaat alles geautomatiseerd. Dat is een van de ontwikkelingen van het internet of things. Wij zijn als overheid bezig om dat sterk te stimuleren. We hebben samen met de Nederlandse werkgevers in de metaalsector fieldlabs opgezet. Dat zijn fysieke omgevingen, waarin verschillende bedrijven al dan niet samen met kennisinstellingen kunnen werken aan internettoepassingen, aan verbindingen van apparaten met internet, aan het benutten van de mogelijkheden daarvan. Daar wordt een heleboel door losgemaakt, waardoor ook kwetsbaarheden aan de orde komen. Het kabinet moet dat, ook samen met het bedrijfsleven, onder ogen gaan zien. Wij zijn nu van plan om samen met dat bedrijfsleven voor die toepassing van het internet of things een roadmap — dat is jargon voor een richtinggevend actieplan — te ontwikkelen. Als we dat hebben, kunnen we samen met het bedrijfsleven kijken hoe we zowel voor de hardware als de software de digitale veiligheid zeker kunnen stellen.

We zijn van plan om al dit jaar met zo'n roadmap te komen. Eerder is al in een motie van de heer Hijink samen met de heer Verhoeven aan het kabinet gevraagd om te onderzoeken welke maatregelen nodig zijn om consumenten te beschermen tegen slecht beveiligde apparatuur. Dit is een van de manieren waarop we ook aan die motie uitvoering geven. Ik ben van plan om voor het eind van het jaar met die roadmap bij de Kamer te komen.

De heer **Hijink** (SP):
Er is volgens mij geen twijfel over de kansen die dit soort apparatuur biedt. Volgens mij zijn we het daar helemaal over eens. Het probleem zit 'm in het volgende. Ik heb het voorbeeld genoemd van de zonnepanelen. Dankzij het werk van een slimme hacker en wetenschapper is blootgelegd hoe makkelijk het is om duizenden pv-systemen tegelijk stil te leggen, met kans op massale uitval van elektriciteit. Dat soort problemen kunnen natuurlijk voorkomen worden als wij veel vaker en veel effectiever testen hoe goed die apparatuur werkt. Daar hebben we geen wetten voor nodig, daar hebben we geen roadmaps voor nodig. Dat kan de regering nu opstarten, samen met de sector, met het bedrijfsleven, met experts, met hackers. Zij kunnen in samenwerking bekijken hoe goed de apparatuur is die in bedrijven en bij consumenten wordt gebruikt. Ga het gewoon testen. Zet mensen in een hokje bij elkaar en ga kijken in welk apparaat we binnenkomen en in welk apparaat niet. Waarom zouden we dat niet doen? Waarom zouden we niet een zwarte lijst aanleggen van apparaten die aantoonbaar slecht zijn, zodat consumenten en bedrijven ook weten: handen daarvan af, dit spul wil je niet in huis?

Minister **Kamp**:
Ik vind de suggesties van de heer Hijink waardevol, maar zijn opmerking dat we die roadmap niet nodig hebben, omdat we met die hackers uit de voeten kunnen, klopt niet. Nee, ik weet niet of hij dat bedoelt. Ik denk dat wij al die dingen moeten doen. Het is nodig om samen met het bedrijfsleven onder ogen te zien wat er allemaal aan risico's zijn en wat je aan beide kanten kunt doen om die risico's te verminderen, om ze weg te nemen of om ervoor te zorgen dat, als ze zich toch manifesteren, je daar adequaat op reageert. Ik denk dat dat nodig is. Ik denk dat het ook nodig is om via ethische hacking, zoals wij dat noemen, te doen wat de heer Hijink zegt. Dat doen we ook. Ons Nationaal Cyber Security Centrum doet dat. De resultaten daarvan zijn van betekenis, maar ik denk dat we het allemaal samen moeten doen. U noemde het voorbeeld van de zonnepanelen die er bij de mensen zijn. Met de omvormers daarvan kunnen zich ook problemen voordoen. Vanwege de contacten die we hebben, vanwege het overleg dat we met elkaar hebben, zien we dat op een gegeven moment ook onder ogen. Het ging specifiek over de omvormers van één fabrikant. Daar is inmiddels een oplossing voor gevonden. Zo gaan we daar iedere keer mee om. De kansen doen zich breed voor, maar de problemen doen zich ook breed voor. We moeten op verschillende manieren op die problemen reageren. Je kunt testen. Je kunt ook mensen erop zetten tegen wie je zegt: "Anderen hacken. Als je voor ons gaat hacken, bekijk dan eens wat de kwetsbaarheid is, zodat we daar wat aan kunnen gaan doen." Ook dat vind ik een reële mogelijkheid om te helpen adequaat te reageren op problemen die zich voordoen of zich voor kunnen doen.

De heer **Hijink** (SP):
Om een misverstand weg te nemen: ik stel niet voor om niet te komen met roadmaps en wetsaanpassingen die echt nodig zijn. Natuurlijk, dat moeten we allemaal doen; het een sluit het ander niet uit. Het punt met de zonnepanelen is, als je de wetenschapper zelf mag geloven, dat het probleem helemaal niet is opgelost. Sterker nog, hij heeft één specifiek merk onderzocht. Ik houd, eerlijk gezegd, mijn hart vast voor hoe het staat met de andere leveranciers van dit soort omvormers. En dan hebben we het alleen nog maar over omvormers. Dan hebben we het nog niet over de botnets die worden aangelegd met op internet aangesloten waterkokers, verlichtingssystemen, stofzuigers en weet ik veel wat. Er wordt zo veel aangesloten aan slecht beveiligde apparatuur dat we volgens mij niet moeten wachten op aanvullende wetgeving om fabrikanten verantwoordelijk te stellen voor de beveiliging van dit soort apparatuur. Dan denk ik dat het voor consumenten kan helpen als er een soort zwarte lijst komt van apparaten waarvan de overheid in samenwerking met experts en hackers heeft vastgesteld dat ze zo lek zijn als een mandje. Dan kan ze zeggen: we kunnen ze nu nog niet bij wet verbieden, maar we maken in ieder geval openbaar dat het geen goede apparaten zijn en dat je ze niet moet gebruiken.

Minister **Kamp**:
Maar wie wacht er nu met wetgeving? Wij niet en u ook niet, want op 1 oktober van dit jaar, vier dagen geleden, hebben we de Wet gegevensverwerking en meldplicht cybersecurity in werking laten treden. We zijn verder druk aan het werk om de Europese richtlijn inzake netwerk- en informatiebeveiliging om te zetten in een implementatiewet. Daar zijn we dus volop mee bezig. Maar wetgeving is één ding. De cultuur is een ander ding. De ontwikkeling rond het internet of things is weer wat anders. Er zijn allerlei apparaten die aan het internet worden gekoppeld, door bedrijven maar ook door particulieren, wat risico's oplevert.

Een voorbeeld daarvan zijn die zonnepanelen. We hebben gesproken over de zelfrijdende auto's. Ik weet dus dat er op een heel breed veld allerlei dingen mis kunnen gaan. Maar ik weet ook dat dit een ontwikkeling is die gaande is in Nederland en in de hele wereld. Die gaat door. We kunnen uit die ontwikkeling heel veel profijt trekken. Dat moeten we er ook uit trekken. Vervolgens moeten we de risico's opsporen, onderkennen en daar adequaat op reageren. Daar ben ik zeer toe bereid. Wij zijn daar zelf, als overheid, zeer toe bereid, niet alleen met wetgeving, maar ook met het Cyber Security Centrum dat we opgericht hebben. Daar bieden we het bedrijfsleven per sector hulp aan door met hen door te nemen waar hun problemen en risico's zitten en door in samenwerking met hen oplossingen te zoeken. Er wordt dus een goede samenwerking tussen alle betrokkenen georganiseerd om de risico's te beheersen.

De heer Hijink sprak ook over de Dragonflysituatie die we hebben meegemaakt. In een aantal landen hebben zich daardoor grote problemen voorgedaan. Er zijn geen berichten dat Nederlandse bedrijven zijn getroffen door die golf van inbreuken op digitale systemen die zich heeft voorgedaan. Maar ik maak me wat dat betreft geen enkele illusie. Zowel individuele hackers als georganiseerde groepen hackers — mensen die het voor de lol doen, mensen die het doen omdat ze er crimineel geld mee willen verdienen — en zelfs staten, zoals mevrouw Bruins Slot zei, houden zich ermee bezig. Dat van die staten is heel reëel. Er zijn staten die zich op grote schaal met dit soort dingen bezighouden. Dat doet zich allemaal voor en we spreken er vanavond over hoe we ons daartegen kunnen beschermen.

De **voorzitter**:
Afrondend, kort.

De heer **Hijink** (SP):
Ja, heel kort. Oké, er gebeurt van alles; laten we het daar dan over eens zijn. Staat de minister vervolgens wel open voor het voorstel dat wij vandaag graag zouden doen dat we, aanvullend op alles wat gebeurt, in ieder geval gaan kijken of we tot een soort zwarte lijst kunnen komen? Het mag wat mij betreft ook anders heten. Ik zou willen dat we actief aan de slag gaan met het testen van bestaande en nieuwe apparatuur, want dat gebeurt op dit moment eigenlijk te weinig. We weten gewoon niet of wat bij mensen in huis hangt, veilig is. Daar hebben we geen regels en wetten voor nodig. Staat de minister open voor zo'n idee?

Minister **Kamp**:
Ik denk dat het belangrijk is om inzicht te hebben en om inzicht te verkrijgen voor zover het er niet is. Het is ook belangrijk om, daar waar je twijfelt, te testen. Ook is het belangrijk om met leveranciers afspraken te maken over de eisen waaraan producten moeten voldoen. Leveranciers dragen ook een eigen verantwoordelijkheid voor de producten die ze leveren. Ik denk dus dat wat de heer Hijink naar voren brengt, heel terecht is. Het moet ook een bijdrage zijn aan de activiteiten die we zullen moeten ondernemen.

Mevrouw **Bruins Slot** (CDA):
De minister verwees er al een paar keer naar dat het heel belangrijk is om de Richtlijn netwerk- en informatiebeveiliging te implementeren. Die brengt namelijk ook een aantal verplichtingen mee voor bepaalde bedrijven en sectoren om zich extra te wapenen tegen hackers en dergelijke. In april van dit jaar hoorden we nog van het kabinet dat deze wet in het najaar van 2017 zou komen. Inmiddels spreekt de minister al van voorjaar 2018. Wat veroorzaakt de vertraging?

Minister **Kamp**:
Ik heb dat zo niet paraat. Ik zal de Kamer daarover informeren. Ik zal nagaan welke toezegging we aan de Kamer hebben gedaan en wat de reden is voor de vertraging die mevrouw Bruins Slot veronderstelt. Ik heb geen reden om aan te nemen dat ze niet weet waar ze over spreekt. Ik zal ook aangeven wat het nieuwe schema is en hoe we dat denken te kunnen halen.

Mevrouw **Bruins Slot** (CDA):
Het was overigens een toezegging aan de Eerste Kamer, die werd gedaan in april 2017. Dat vergemakkelijkt het zoeken misschien wat.

Minister **Kamp**:
Dank u. Ik zal het nagaan.

Dan ben ik gekomen bij de zaken die mevrouw Bruins Slot naar voren heeft gebracht. Zij vraagt zich af hoe wij als overheid voortdurend geïnformeerd blijven over de ontwikkelingen die er zijn. Het is voor ons een heel belangrijke opgave om te weten wat er gebeurt en om zelf bij te houden hoe het zit met de relevante wet- en regelgeving. Is die voldoende of behoeft die aanvulling? Ik heb hier al gezegd hoe we daar nu mee bezig zijn. Mevrouw Bruins Slot gaf zonet zelf al aan wat het vervolg is in de implementatiewet van de Europese richtlijn. Die ontwikkelingen gaan snel. Er zijn ook overheidsonderdelen die als taak hebben om dat te volgen. Een daarvan is de ACM en een andere is het Agentschap Telecom. Zij hebben toezichtsbevoegdheden. Dat betekent dat zij ook degenen zijn die in gesprek zijn met het bedrijfsleven. Ik heb het net gehad over het Nationaal Cyber Security Centrum. Dat is weer onderverdeeld in zogenaamde ISAC's. Dat zijn publiek-private samenwerkingsverbanden per sector. Daarin wordt, zoals ik net heb toegelicht, gezamenlijk met het bedrijfsleven gekeken wat er allemaal speelt en wat er gedaan moet worden. Ik heb zonet tegen een van de andere woordvoerders gezegd dat ik met de sector en met de toezichthouders over specifiek de elektriciteitsvoorziening een conferentie zal organiseren, waaruit ik acties zal laten voortkomen. Ik zal kijken hoe ik dat model ook op andere sectoren kan toepassen, aanvullend op wat ik zonet al heb gezegd.

De ethische kwesties heeft mevrouw Bruins Slot zeer terecht aan de orde gesteld. Die spelen volop. Wat de heer Jetten zei over de algoritmen, sluit daarbij aan. Ik heb zo niet beschikbaar wat er op dit moment allemaal bij de rijksoverheid speelt op het punt van algoritmes. Er zijn algemene verantwoordelijkheden waar bedrijven zich aan moeten houden. Wat algoritmes betreft is er niet specifiek iets waar we aparte wettelijke bepalingen voor moeten opnemen

naar mijn overtuiging. Het is iets wat je meer in algemene zin kunt regelen. Ik ben het met de heer Jetten eens dat algoritmes steeds meer toegepast worden en ook heel nuttig zijn, maar dat zij ook risico's met zich meebrengen omdat er ethische kwesties aan verbonden zijn. Dus het lijkt me nuttig om eens te kijken wat daar speelt en wat we daar mee moeten. Ik weet nog niet wie daar het initiatief voor moet nemen en hoe we dat vorm moeten geven. Maar het onderwerp is door de heer Jetten geagendeerd en ik zal het de aandacht geven die de heer Jetten vraagt. Ik ben van plan om nog voor de behandeling van de begroting van Economische Zaken de Kamer op dit punt te informeren, zodat de heer Jetten daar desgewenst bij de begrotingsbehandeling verder op in zou kunnen gaan.

De heer **Jetten** (D66):
Veel dank voor de toezegging van de minister. Ik heb misschien een korte aanvulling. Ik kan me voorstellen dat het interessant is om dat bijvoorbeeld samen met de VNG te doen, juist omdat veel gemeenten worstelen met de vraag hoe zij algoritmes op een goede manier kunnen inzetten. Als Rijk en lokale overheden elkaar daarin kunnen versterken, zou dat mooi zijn.

Minister **Kamp**:
Die suggestie neem ik ook graag mee, mijnheer de voorzitter.

De heer Bosman sprak over de infrastructuur, met name de energie-infrastructuur. Ik weet dat energie een grote hobby van hem is. Ik heb een aantal gelegenheden gehad om daar met hem in ander verband over te spreken. Ik heb net al wat gezegd over de NCSC, het Nationaal Cyber Security Centrum. Bij wet is vastgelegd dat het Nationaal Cyber Security Centrum optreedt als een computer emergency response team. Dat betekent dat zij ook weer hun vaardigheden ter beschikking moeten stellen in de vorm van een expertise- en adviescentrum voor wat betreft ontwikkelingen op het punt van cyber security aan het bedrijfsleven en anderen die digitale voorzieningen gebruiken. Ik geloof dat het niet alleen op het punt van energie maar breed van grote betekenis is dat we dat doen.

Voorzitter, ik kijk of ik op de punten van de heer Jetten ben ingegaan. Hij sprak over auto's, waar ik op in ben gegaan, en over algoritmes. Hij sprak over de kansen en uitdagingen. Ik denk dat dit is gebeurd en ik dank u voor de gelegenheid om te mogen reageren op hetgeen de woordvoerders in de eerste termijn naar voren hebben gebracht. Dank u wel.

De **voorzitter**:
U bedankt. Een vraag nog van de heer Jetten.

De heer **Jetten** (D66):
Dank aan de minister voor de uitgebreide toelichting op bijna al mijn punten. Ik had nog een concrete vraag. Is de minister het met mij eens dat het interessant zou zijn om ook bij de rijksoverheid bug challenges te organiseren waarbij wij hackers uitnodigen om de systemen van de rijksoverheid eens flink door te lichten? Op die manier kunnen we preventief kijken waar we het een en ander kunnen versterken.

Minister **Kamp**:
Daar heb ik net al het nodige over gezegd. Ik heb gezegd dat bij het Nationaal Cyber Security Centrum er ook ethisch hacking plaatsvindt. Ik zal kijken in hoeverre dat overeenkomt met de suggestie die de heer Jetten heeft gedaan en in hoeverre een aanvulling daar nog zinvol is. Daar kom ik in het stuk waar ik net over gesproken heb, dat nog voor de begroting naar de Kamer zal gaan, nader op terug.

Misschien mag ik in de richting van mevrouw Bruins Slot meteen laten blijken dat ik ook zeer geholpen wordt door mijn medewerkers die mij over de implementatie van de NIB-richtlijn aanreiken dat het wetsvoorstel klaar is. Het is in consultatie geweest. Het zal zo spoedig mogelijk in de ministerraad worden gebracht. Het lijkt mij het beste om dat in de nieuwe ministerraad te doen, maar ik zal er nog even naar kijken. Afhankelijk van het tempo van behandeling in de Tweede en Eerste Kamer acht ik het mogelijk dat we de wet voor de zomer van 2018 al in werking kunnen laten treden. Ik denk dat dat in overeenstemming is met het tijdschema dat mevrouw Bruins Slot net noemde, zodat we op dat punt geen nader huiswerk van haar hebben gekregen.

Dank u wel, mijnheer de voorzitter.

De **voorzitter**:
Heel goed, weer een geruststelling voor ons als Kamer.

Ik stel vast dat er behoefte is aan een tweede termijn. Wij gaan luisteren naar de heer Van der Lee van de fractie van GroenLinks. Hij heeft, zoals iedereen, één minuut spreektijd.

De heer **Van der Lee** (GroenLinks):
Hartelijk dank, voorzitter. Ook veel dank aan de bewindspersoon voor de uitgebreide beantwoording. Ik respecteer volledig zijn diep demissionaire positie. Daarom wil ik de collega's een motie voorleggen om zich ergens over uit te spreken.

De **voorzitter**:
Dat is toch bij elke motie het geval?

De heer **Van der Lee** (GroenLinks):
De motie luidt als volgt.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat digitalisering enorme kansen biedt voor duurzame groei, maar onze vitale infrastructuur en belangrijke publieke waarden steeds kwetsbaarder maakt;

overwegende dat dit tot belangrijke uitdagingen leidt in vrijwel alle maatschappelijke domeinen waarin de overheid actief is;

spreekt uit dat het instellen van een digitale onderraad wenselijk is voor zowel het volop benutten van digitale kansen als het borgen van publieke waarden en vitale belangen,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 492 (26643).

Mijnheer Van der Lee, blijft u nog even staan, want er is een vraag van de heer Hijink.

De heer **Hijink** (SP):
Ik vraag mij af waarom de heer Van der Lee ervoor kiest om niet conform het advies van de commissie-Elias te gaan voor één minister die verantwoordelijkheid draagt voor het ICT-beleid. Waarom kiest hij voor een afzwakking daarvan?

De heer **Van der Lee** (GroenLinks):
Omdat ik van mening ben dat het heel ingewikkeld is om één persoon eindverantwoordelijk te maken voor digitalisering in al haar consequenties. Digitalisering raakt alle domeinen waarop de overheid actief is en alle maatschappelijke sectoren. Het is straks de infrastructuur achter de infrastructuren. Daar zal een collectieve verantwoordelijkheid onmiskenbaar een rol spelen. De opgave zit waarschijnlijk vooral in uitstekende coördinatie, goed onderling overleg en adequate agendering, ook van vraagstukken waar één persoon niet altijd onmiddellijk alles van zal afweten. Dat zal een veel betere borging bieden dan in het geval dat één persoon verantwoordelijk gemaakt wordt.

De heer **Hijink** (SP):
Maar juist dan ligt het toch voor de hand dat één bewindspersoon daar de eindverantwoordelijkheid voor draagt? Het een hoeft het ander toch niet uit te sluiten?

De heer **Van der Lee** (GroenLinks):
Het lijkt mij in die zin goed dat die onderraad één voorzitter heeft, maar ik weet eerlijk gezegd niet goed welke bewindspersoon dat zou moeten zijn. Je kunt een argumentatie bedenken op grond waarvan het de minister van Economische Zaken zou moeten zijn, of van I en M, of Binnenlandse Zaken, of misschien wel Defensie, gelet op de risico's op het vlak van cybersecurity. Dat vind ik een heel ingewikkeld vraagstuk. Om die reden leg ik geen specifiek verzoek tot het doen van een uitspraak voor.

De **voorzitter**:
Dank u wel. Dan is het woord aan de heer Hijink van de SP-fractie.

☐

De heer **Hijink** (SP):
Voorzitter. Ik wil alleen één motie indienen.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat kwetsbaarheden in apparatuur die verbonden zijn met het internet tot grote schade kunnen leiden voor particulieren, bedrijven en de samenleving;

overwegende dat de Kamer eerder de regering heeft verzocht om aanvullende maatregelen te onderzoeken om Internet of Things (IoT)-apparatuur beter te beveiligen;

verzoekt de regering — in samenwerking met het bedrijfsleven, cybersecurityexperts en hackers — hacktests te laten uitvoeren op IoT-apparatuur en voorts een lijst te publiceren van onveilige apparaten,

en gaat over tot de orde van de dag.

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

Zij krijgt nr. 493 (26643).

De **voorzitter**:
Het woord is aan de heer Jetten van de fractie van D66.

☐

De heer **Jetten** (D66):
Voorzitter, dank u wel. Dank aan de minister voor de uitgebreide beantwoording en de wijze waarop hij bij de verschillende dilemma's heeft stilgestaan. Dank ook voor de toezegging om te kijken in hoeverre wij nu binnen de overheid algoritmes gebruiken en welke dilemma's daar eventueel bij naar voren komen.

Tot slot wil ik nog even terugkomen op een punt waarop de minister uitgebreid is ingegaan in zijn beantwoording, namelijk de zelfrijdende auto's. Ik ben het helemaal met hem eens dat Nederland op dit vlak een kopland is. Wij proberen met open vizier, bijvoorbeeld rondom Eindhoven en Helmond, alle uitdagingen van die rijdende auto's te ontdekken. Volgens mij is dat ook de houding die wij op al die thema's moeten hebben: kijken naar de kansen van digitalisering, maar wel altijd kritisch, en ervoor zorgend dat wij dit op een goede manier een plek geven in onze samenleving.

De **voorzitter**:
Ik stel vast dat mevrouw Bruins Slot afziet van haar spreektijd. Hetzelfde geldt voor de heer Bosman. Daarmee zijn wij gekomen aan het eind van de tweede termijn van de Kamer. Ik begrijp dat de minister nu reeds kan antwoorden en de moties kan becommentariëren.

☐

Minister **Kamp**:
Voorzitter. De motie op stuk nr. 492 van de heer Van der Lee spreekt uit dat het instellen van een digitale onderraad

wenselijk is voor "zowel het volop benutten van digitale kansen als het borgen van publieke waarden en vitale belangen". Ik vind het niet gepast dat ik daar als demissionaire minister iets over zeg terwijl dat organisatorische punt door het volgende kabinet in de ministerraad moet worden ingevuld. Ik wil aan die vrijheid van de volgende ministerraad niets afdoen. Ik merk nog even naar de heer Van der Lee op dat ik het met hem eens ben dat er coördinatie moet plaatsvinden als er zo'n onderraad zou komen. In de huidige structuur kan één minister geen voorzitter zijn van zo'n onderraad, want in de huidige structuur zit de minister-president alle onderraden voor. Het is wel denkbaar dat een van de andere ministers op verzoek van de minister-president een zekere coördinerende rol vervult. Ik heb eigenlijk liever dat de Kamer zo'n uitspraak doet richting het nieuwe kabinet. Dat lijkt me gepaster. Anderzijds realiseer ik mij dat het heel goed mogelijk is dat het kabinet al besluiten op dit punt neemt voordat de Kamer zich dat goed en wel bewust is. Met die overweging laat ik het oordeel aan de Kamer. Ik benadruk nog een keer dat ik niet van plan ben om mijn opvolgers en het volgende kabinet op dit punt voor de voeten te lopen, maar ik laat het aan de Kamer om daar nu wel of niet een uitspraak over te doen.

In de motie op stuk nr. 493 vraagt de heer Hijink om in samenwerking met het bedrijfsleven hacktesten te laten uitvoeren en een lijst te publiceren van onveilige apparaten. Ik vind het testen door hackers van systemen, van software en hardware, nuttig. Dat gebeurt ook al. De aandacht die de heer Hijink daarvoor vraagt, vind ik niet verkeerd. Ik vind wel dat aan het publiceren van een lijst van onveilige apparaten een heleboel haken en ogen zitten. Dat kun je niet zomaar doen. Er zijn verschillende gradaties in "veilig" en "onveilig". Als je iets onveilig verklaart, zou het zo kunnen zijn dat men overgaat op vergelijkbare dingen die nog niet getest zijn en toch ook weer onveilig zijn. Daar zitten dus een heleboel dingen aan vast. Ik denk daarom dat dit te vroeg is. Als de motie alleen een verzoek zou zijn aan de regering om in samenwerking met het bedrijfsleven hacktests onderdeel te laten zijn van ons beleid, dan heb ik daar geen bezwaar tegen. Dan zou ik het oordeel aan de Kamer laten. Als erin blijft staan dat het een lijst moet zijn met onveilige apparaten, ontraad ik deze motie. Dat is de tekst die op dit moment voorligt, dus de motie op stuk nr. 493 ontraad ik.

Ik kan mij vinden in wat de heer Jetten zei.

Voor het overige dank ik de Kamer voor de steun die gegeven wordt. Er zal op dit punt een heleboel moeten gebeuren. De kansen die er zijn, zullen we moeten pakken. De uitdagingen en problemen die er zijn, zullen we moeten aanpakken. Daarvoor is een heleboel werk te doen, maar als we dat goed doen, kan het de samenwerking echt weer een eind vooruit helpen.

Dank u wel, mijnheer de voorzitter.

De beraadslaging wordt gesloten.

De **voorzitter**:
Dank aan deze diep demissionaire minister voor zijn aanwezigheid hier vandaag.

Wij stemmen aanstaande dinsdag over beide moties.