37
Buitenlandse spionage via mobiele netwerken

Aan de orde is het **debat** over **buitenlandse spionage via mobiele netwerken**.

De **voorzitter**:
Dames en heren, we gaan beginnen. We gaan het debat voeren over de buitenlandse spionage via mobiele netwerken. Ik kijk even naar de deelnemers. Ik wil graag met u afspreken om drie interrupties toe te staan. Ik zie geen reactie, maar dat gaan we gewoon doen. Allereerst geef ik het woord aan mevrouw Van Ginneken van D66.

Mevrouw **Van Ginneken** (D66):
Dank u wel, voorzitter. In 2009 kijken onderzoekers op verzoek van KPN naar risico's voor ongewenste inmenging in het telecomnetwerk. Ze schrijven een alarmerend rapport. Huaweipersoneel kan ongeautoriseerd, ongecontroleerd en onbeperkt mobiele nummers van KPN-gebruikers afluisteren, vanuit KPN-gebouwen in Nederland, maar ook vanuit China. En ze kunnen meer.

Voorzitter. Veilige en vertrouwelijke communicatie is een fundament van onze samenleving. Het is niet voor niets een grondrecht. Je moet vertrouwen kunnen hebben dat er niemand meeluistert als je een telefoongesprek voert. Dat is essentieel voor journalisten, voor onderzoekers, voor mensenrechtenactivisten, voor bedrijven, en zo kan ik nog wel doorgaan, want het is essentieel voor ons allemaal. Als bedrijven en onderzoekers onderling niet vrijuit over hun innovaties en nieuwe kennis kunnen spreken, als kritische journalisten en mensenrechtenactivisten zich via de telefoon niet veilig kunnen voelen, dan valt een basis onder onze samenleving weg. Daarom wil ik van de staatssecretaris horen of ze doordrongen is van deze risico's en of ze de juiste maatregelen neemt om de kwetsbaarheden ook snel op te lossen.

Voorzitter. Op mijn verzoek stuurde de staatssecretaris ons in juni een brief waarin ze schetste wat er gedaan is en nog gedaan moet worden om ons telecomnetwerk veiliger te maken. Maar er lijkt een gat te zitten in dit cv van de staatssecretaris. De staatssecretaris heeft sinds december 2019 al de bevoegdheid om een aanwijzing te geven om niet-vertrouwde bedrijven te weren uit kritieke delen van het telecomnetwerk. Toch had de staatssecretaris dat nog niet gedaan toen de Volkskrant in april haar artikel publiceerde. Een paar weken later hoorden we in het commissiedebat dat de beschikkingen waarin die aanwijzingen staan, net verstuurd waren. Ik kan me daarom niet aan de indruk onttrekken dat de staatssecretaris pas in actie is gekomen nadat de Volkskrant hierover publiceerde en ik hierover vragen stelde tijdens het vragenuur van 20 april, dus daarom mijn vraag: waarom heeft de staatssecretaris vijftien maanden gewacht voordat zij de beschikkingen verstuurde?

Voorzitter. De belangrijkste vraag is natuurlijk: vanaf wanneer kan de samenleving erop rekenen dat we weer veilig en vertrouwelijk kunnen communiceren? Ik stoor me eraan dat heel veel informatie hierover vertrouwelijk is verklaard en dat ik via de krant soms meer te weten kom, bijvoorbeeld over compensatie, zoals in het artikel van het FD van vanochtend. Daarom vraag ik aan de staatssecretaris: welke termijn heeft zij aan de mobiele netwerkoperators gesteld om het netwerk op te schonen? Hoe weten we als Kamer en als samenleving of die opschoning ook op tijd en goed is uitgevoerd? Wordt er compensatie geboden aan de mobiele netwerkoperators? En kan de staatssecretaris openbaar maken wat het onderscheid is tussen kritieke en niet-kritieke delen van het netwerk en of we daarmee voldoende veiligheid inbouwen?

Tot slot, voorzitter. Ik zou graag met de staatssecretaris uitgebreid van gedachten wisselen over wat we als Nederland en Europa kunnen doen om minder afhankelijk te worden van niet-Europese techleveranciers, maar ik hoop dat op een ander moment te doen, want daar is nu te weinig tijd voor. Wellicht kan een van mijn collega's daar vanavond toch alvast stiekem een beginnetje mee maken, dus ik doe hierbij de uitnodiging. Ik kijk uit naar de beantwoording van mijn vragen door de staatssecretaris.

Dank u wel.

De **voorzitter**:
Dank u. Dan geef ik het woord aan mevrouw Leijten van de SP.

Mevrouw **Leijten** (SP):
Voorzitter. Bij het voorbereiden van dit debat, waarin het gaat om techniek, achterdeurtjes, spionage, grote belangen, mensenrechtenbelangen, bedrijfseconomische belangen en de handelsrelatie met China, vroeg ik mij voornamelijk af waarom wij in hemelsnaam voor onze infrastructuur, die zo van wezenlijk belang is voor ons dagelijks leven, voor de veiligheid in ons land en voor de communicatie die we hebben, afhankelijk zijn van private bedrijven die ook in handen kunnen zijn van staten waarvan wij zeggen: dat is een groot risico. Dat is historisch natuurlijk zo gegroeid. De telefoniemarkt is een markt geworden, maar de technologie heeft de vraag "organiseren we dat nou wel op de juiste manier?" eigenlijk ingehaald. De technologie, waarbij we dingen vertrouwen en dingen die door anderen gezien kunnen worden met elkaar delen, met alle risico's van dien, is helemaal niet zo veilig. Mijn vraag is: kunnen we het nou repareren? De staatssecretaris kan allemaal dingen aanwijzen en bepaalde organisaties of ondernemingen uit bepaalde ontwikkelingen halen. Denk bijvoorbeeld aan de uitrol van 5G. Daarvan hebben we al gezegd: we willen niet meer dat Huawei daar een rol in speelt. Maar waarom doen we het niet zelf? Waarom kunnen wij dat als land in de Europese Unie — we kunnen ook samenwerken met landen — niet zelf opzetten? Zijn daar ideeën over? Zijn er voorbeelden in de wereld waarbij dat wel wordt gedaan, zo vraag ik de staatssecretaris.

De afhankelijkheid van private partijen voor cruciale infrastructuur is niet altijd veilig. Wij hebben het ook heel vaak gehad over staatsgeheime documenten. Waar worden die nou bewaard? Dat gebeurt bij een organisatie die nu is overgenomen door een Britse bv. Daar hebben wij vragen over gesteld. D66 heeft daar ook vaak vragen over gesteld. Dan is het antwoord eigenlijk altijd: nee, het is nog wel veilig, want het ligt nog in Nederland. Maar zijn onze

staatsgeheime documenten uiteindelijk nog van ons? Daar hoeven we niet per se vandaag een antwoord op te hebben, maar het laat wel zien hoe we misschien in een situatie terecht zijn gekomen waarin we echt een visie moeten gaan ontwikkelen. Dat sluit misschien een beetje aan bij de oproep van mevrouw Van Ginneken van D66. Waar vinden wij nou dat de grenzen van publiek en private waarborgen liggen? Waar moeten wij mogelijk een inhaalslag maken en dingen zelf gaan doen? Ik zou graag van de staatssecretaris daar een bespiegeling op horen.

We zien dat de digitale samenleving niet meer weggaat. Die gaat zich alleen nog maar versnellen. Tot in de haarvaten van de zorg, het onderwijs en ons eigen contact: het zit overal. Daarmee is de rol van de overheid daar natuurlijk ook gewoon bij aanwezig. De overheid is namelijk medeverantwoordelijk voor de bescherming van ons allemaal. Dat is in al die ontwikkelingen misschien niet echt ontwikkeld. Waar sta je en wat moet je dan regelen? Ik vraag de staatssecretaris dus of zij bereid is om zo'n visie te maken.

Mevrouw **Van Ginneken** (D66):
Mevrouw Leijten refereert aan het voorzetje dat ik gegeven heb. Ik vind het wel van belang om even te benadrukken dat dat voorzetje niet ging over de vraag of we delen van de telecominfrastructuur misschien meer in publieke handen moeten gaan trekken, maar over het idee om onszelf onafhankelijker te maken van technologieleveranciers van buiten Europa. Dat wil ik in elk geval even gememoreerd hebben.

Mevrouw **Leijten** (SP):
Maar dan zou mijn antwoord zijn: als je het op die manier wil knippen, dan maak je nu misschien een probleem van Chinese staatsbedrijven, maar het kan natuurlijk ook een Israëlisch bedrijf zijn dat gelieerd is aan de Israëlische veiligheidsdienst, of een Amerikaans bedrijf waarvan wij eigenlijk niet willen dat onze gegevens daar in handen zijn. We hebben een groot en breed debat als het gaat over de invloed van de grote technologische bedrijven op ons leven, op algoritmes en op wat ze aanbieden, maar daaronder zit wat de SP betreft wel degelijk het vraagstuk: wat regelen we nou zelf publiek en wat privaat? Ik zie waar we staan: alles is privaat, overal. Er gaan heel veel subsidies heen om het veilig te maken, maar als je dan een veilige contractpartner hebt en die vervolgens wordt overgenomen, heb je daar toch geen zeggenschap over. En wat gebeurt er dan? Dan kom je wel degelijk bij de vraag die ook D66 in het verleden heeft gesteld — dat was uw voorganger de heer Verhoeven — namelijk: wat doen we bijvoorbeeld met Fox-IT? Dat is nu overgenomen door een buitenlandse partij. Daarbij valt cruciale informatie van onze Staat wellicht in handen … Het gaat om staatsgeheimen, dus dat moet in een kluis, dat is een digitale kluis. Maar weet je zeker dat dat goed gaat? Dus daarom heb ik 'm wel verbreed.

De **voorzitter**:
Dank. Dan geef ik het woord aan mevrouw Kathmann van de PvdA.

Mevrouw **Kathmann** (PvdA):
Dank u, voorzitter. Mijn collega van D66 zei het al: we staan hier niet voor niks. We hebben het hier namelijk over de conclusies van het rapport waarvoor dit debat is aangevraagd. Ik zal er een citeren: "De bevindingen van het interne rapport waren zo explosief dat werd gevreesd voor het lot van KPN Mobiel als die zouden uitlekken." In het rapport staat: "Het voortbestaan van KPN is ernstig in gevaar omdat mogelijk vergunningen worden ingetrokken of overheid en bedrijfsleven hun vertrouwen in KPN opzeggen indien bekend wordt dat de Chinese overheid ongecontroleerd mobiele KPN-nummers kan afluisteren en het netwerk kan platleggen." Steeds als ik die zin lees, dan schrik ik. Ik denk dat mevrouw Leijten er namelijk gelijk in heeft dat digitale infrastructuur een nutsvoorziening is en dat digitale connectiviteit een mensenrecht is. Dat vraagt om een hele sterke overheid die bereid is om haar burgers te beschermen. Het is ook heel normaal dat we buitenlandse mogendheden niet onze wegen laten monitoren. Want zie je het al voor je? De overheid van een ander land die precies weet hoeveel auto's er over onze wegen rijden, wie er in die auto zitten en waar ze heen gaan. Het is al bizar als we dat zelf als overheid allemaal zouden weten. Toch geven we de overheden van sommige landen toegang tot onze digitale snelwegen. We laten ze zien wie benadert en wat onze bedrijven doen. Het is daarom logisch dat de regelgeving een paar jaar geleden is verbeterd en dat onze mobiele providers in 2022 weerbaar moeten zijn voor buitenlandse spionage. Kan de minister vertellen hoe het ervoor staat? Zijn die bedrijven ook echt al weerbaar in de praktijk?

De PvdA vraagt zich echter af of het niet veel logischer is om technologie van bedrijven uit landen die we niet vertrouwen helemaal te weren. Om in de snelwegmetafoor te blijven: ook als we er regels voor bedenken, is het onacceptabel om de snelwegen te laten monitoren door mogendheden die we niet vertrouwen. Zelfs als er regels aan verbonden zijn, wil ik helemaal niet dat een buitenlandse overheid weet waar ik heen rijd.

De afgelopen jaren heeft de overheid enkele afritten beter beschermd, maar België gaat een stap verder. Daar zijn die bedrijven van mogendheden die we niet vertrouwen bijvoorbeeld helemaal niet welkom in de haven van Antwerpen. In het Verenigd Koninkrijk, in Zweden en in Spanje gaan ze nóg een stapje verder. Daar worden bedrijven van niet-vertrouwde mogendheden volledig geweerd uit de digitale infrastructuur. Hoe beoordeelt de minister de stappen die deze landen hebben gezet? Denkt de minister niet dat het beter is dat bepaalde bedrijven volledig worden geweerd ten behoeve van onze veiligheid? En wat zouden de gevolgen daarvan zijn? Op dit punt overweegt de Partij van de Arbeid ook een motie.

Natuurlijk is het niet mogelijk om als Nederland alles zelf te doen. Het is van groot belang dat in heel de EU de digitale veiligheid gewaarborgd is. In Europa moeten we een goed alternatief kunnen bieden voor de marktmacht van bijvoorbeeld Chinese techbedrijven, zodat we niet meer afhankelijk zijn van bedrijven die we niet vertrouwen op plekken waar het borgen van onze veiligheid cruciaal is. Bent u bereid — dat zeg ik via u, voorzitter — om in Europees verband te pleiten voor het eventueel weren van bedrijven en landen die we niet vertrouwen op cruciale plekken in onze digitale infrastructuur?

De **voorzitter**:
Dank u. Dan ga ik naar de volgende spreker. Dat is mevrouw Rajkowski van de VVD.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Als je belt, wil je niet dat jouw telefoontje wordt afgeluisterd. Wat je bespreekt met elkaar is privé en dat moet ook zo blijven. Dus als je belt met je vriendin Jasmijn, of met familie, of als ministers bellen met elkaar over belangrijke zaken als de nationale veiligheid, is het belangrijk dat dit privé blijft. In Nederland moeten we kunnen rekenen op goede telecommunicatienetwerken, zodat we veilig verbonden zijn. Daar werken alle telecomaanbieders in Nederland aan. Sterker nog, onze Nederlandse netwerken behoren tot de beste, veiligste en innovatiefste netwerken van de wereld. Daar mogen we best trots op zijn. Wat wij met elkaar in Nederland bespreken kan echter ook interessant zijn voor mensen uit andere landen. We hebben in Nederland namelijk bedrijven die zulke gespecialiseerde kennis hebben dat die uniek is, niet alleen in Nederland, maar ook in de wereld. Kennis die voor anderen, bijvoorbeeld China, erg interessant is om te hebben.

Voorzitter. We moeten onze Nederlandse telecomnetwerken beschermen tegen kwaadaardige invloeden van buitenaf. We moeten ze beschermen tegen statelijke dreigingen. We worden hier dagelijks voor gewaarschuwd. Landen zijn geïnteresseerd in onze kennis. Wij doen in Nederland hele gave dingen met hele slimme mensen, die niet alleen de wereld innoveren maar ook een boost geven aan de bv Nederland, waar we allemaal van profiteren. Daarnaast zijn er ook landen die onze sterke democratie schade willen toebrengen. Sommigen denken dat dit wel meevalt en dat dit spookverhalen zijn, maar helaas, het nieuws over het rapport uit 2010 van Huawei en KPN en eerder ook Telfort maakt dat de vrees voor afluisterpraktijken toch gegrond is. We moeten dus ook niet naïef zijn en denken dat niemand interesse heeft in onze telecomnetwerken. De VVD heeft de afgelopen jaren vaker in debatten over 5G gevraagd om een aantal maatregelen. Aan de hand daarvan zijn een aantal stappen gezet om het netwerk veiliger te maken. Daar wil ik de staatssecretaris dan ook voor bedanken.

De hoofdvraag is nu: zijn we in control en doen we er alles aan om de kans zo klein mogelijk te maken dat anderen kunnen meeluisteren? Daar heb ik een aantal voorstellen voor. In 2019 heeft de Taskforce Economische Veiligheid een risicoanalyse uitgevoerd en gekeken hoe kwetsbaar onze telecommunicatienetwerken zijn voor misbruik van technologische leveranciers. Ik wil inzicht hebben in die kwetsbaarheid van onze netwerken nadat nieuwe maatregelen zijn uitgevoerd. Daarom wil ik aan de staatssecretaris vragen om een nieuwe risicoanalyse wanneer alle nieuwe maatregelen zijn uitgevoerd.

Het tweede is: wat als we de kern van onze netwerken afsluiten voor mensen die kwade bedoelingen hebben en misschien voor specifieke partijen, maar de rest van het netwerk wel in handen is van diezelfde partijen? Dan is misschien het kritieke onderdeel wel beveiligd, maar zijn we alsnog afhankelijk. Het is precies die strategische afhankelijkheid waar we voor gewaarschuwd worden. In andere landen wordt het RAN-deel wel als kritisch netwerk gezien, in Nederland niet. RAN is de link tussen het netwerk en de telefoons, dus antennes en basisstations. Als alle grote telecompartijen dus hun RAN maar bij één buitenlandse partij draaien, worden we dan niet toch weer te afhankelijk? Kan de staatssecretaris hierop reageren? Misschien is dit wel een mooi punt om ook mee te nemen, mocht de taskforce zijn nieuwe risicoanalyse weer gaan uitvoeren.

Voorzitter. Dan end-to-end-encryptie. Dat is een belangrijke ontwikkeling die onze communicatie steeds veiliger houdt. Dit gaat het afluisteren veranderen, zo niet haast onmogelijk maken. Wat betekent dit voor hoe mensen met kwade bedoelingen alsnog binnen willen komen en nieuwe informatie willen krijgen? Op welke punten wordt het netwerk dan interessant? Zijn we daar ook tegen beveiligd?

Voorzitter. Als het gaat om onze nationale veiligheid, dan zijn het onze inlichtingen- en veiligheidsdiensten zoals de AIVD — ik weet dat die onder een andere minister valt — die samenwerken met onze telecomproviders. Maar hoe ziet die samenwerking er dan uit? Als de AIVD constateert dat bedrijf X niet meer kan, iedereen naar bedrijf Y gaat en later blijkt dat bedrijf Y ook niet meer kan, bij wie ligt dan de verantwoordelijkheid? Wat is het verschil tussen overheid en bedrijfsleven samen?

Voorzitter, mijn laatste zin. Ik heb nu een aantal voorstellen gedaan om te kijken hoe we ons netwerk nog veiliger kunnen maken, juist zodat we strategisch onafhankelijk blijven en onze bedrijven met unieke producten en hoogtechnologische kennis kunnen beschermen.

Dank u wel.

De **voorzitter**:
Dank u. Er is een interruptie van de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Dank voor de inbreng van de VVD. Op zich een helder verhaal, maar ik mis een beetje een antwoord op de vraag wat nou de verantwoordelijkheid is van de private sector in dezen. Ik ga zelf ook niet zo ver dat ik denk: je moet al die infrastructuur in publieke handen brengen. Dat kunnen we ook eigenlijk niet, publiek, denk ik, niet op het niveau dat je zou willen. Maar je ziet wel — en dat is mede VVD-beleid — dat de enorme concurrentie die wij bevorderd hebben tussen telecomproviders ertoe geleid heeft dat marketingafdelingen groeien, maar dat er bezuinigd wordt op de technische deskundigheid en daarmee op het vermogen om goed te beoordelen wat financiers leveren, wat daarin de gaten zijn en hoe we ons beter kunnen beschermen. Erkent de VVD dat en welke verantwoordelijkheid zou zij willen beleggen bij de marktpartijen in dezen?

Mevrouw **Rajkowski** (VVD):
Als het gaat om de telecomnetwerken, zijn onze marktpartijen er ook verantwoordelijk voor dat wij met z'n allen veilig kunnen communiceren via hun telecomnetwerken. Volgens mij doen ze daar ook van alles aan. Op het moment dat een telecomnetwerk ... Misschien is er wel een aanbesteding en komt er een partij: hé, dat is interessant. Misschien zit daar wel een land achter, misschien zit China erachter, dat denkt: als wij nou met een hele lage prijs, een laag tarief komen, dan winnen wij de aanbesteding. De vraag die dan

optreedt is: als iemand met een laag tarief probeert binnen te komen, weten de telecomaanbieders dan ook welke redenen daarachter zitten? Het is niet altijd zo ... Dat bedoelde ik net met bedrijf X en Y, om even geen namen te noemen. Apparaten die nu in bepaalde systemen zitten moeten misschien vervangen worden. Maar het is niet zo dat toen die ooit aangeschaft werden, iedereen dacht: o, maar daar zit China achter of een ander land, maar weet je, het is lekker goedkoop; deze gaan we lekker kopen. Zo denken die telecomnetwerken niet. Ik snap eigenlijk niet zo goed waar deze vraag vandaan komt. Ik ben ervan overtuigd dat onze telecomaanbieders er alles aan doen om een zo veilig mogelijk netwerk te kunnen aanbieden. Want op het moment dat het niet veilig is, hebben zij ook een groot probleem.

De heer **Van der Lee** (GroenLinks):
Het verbaast me dat de VVD dat niet snapt. De VVD wil graag concurrentie bevorderen. We veilen frequenties. We willen daar geld uit halen, ook als overheid. Maar we willen ook dat ze flink concurreren in de markt. In de visie van de VVD willen Nederlanders de beste technologie voor de laagste prijs, maar dat leidt natuurlijk ook tot een bepaald gedrag in het aankopen van apparatuur door die telecombedrijven. Als je wil dat het veiliger is, dan moet de VVD ook bereid zijn te accepteren dat de prijzen waarschijnlijk toch iets hoger zullen worden. Als je die kwaliteit, die veiligheid wil borgen, dan heb je de technische knowhow en ook de capaciteit nodig om dat goed te kunnen beoordelen. Daar gaat mijn vraag over.

Mevrouw **Rajkowski** (VVD):
Ja, dank. Ik denk dat we het daar met elkaar over eens zijn in die zin dat de laagste prijs niet altijd betekent dat je daarmee het veiligst bent. Kijk bijvoorbeeld naar Facebook. Iedereen denkt: o, dat is gratis. Dat is niet gratis; je betaalt alleen met wat anders. Ik denk dat het goed is dat we juist die naïviteit wat meer naar voren brengen in het debat. Voor dit soort vitale infrastructuur is de laagste prijs niet altijd het beste voor het land.

De **voorzitter**:
Dank u. Dan ga ik over naar de volgende spreekster. Dat is mevrouw Van Dijk van het CDA.

Mevrouw **Inge van Dijk** (CDA):
Dank u wel, voorzitter. Onze Jip van 11 kwam afgelopen woensdag bij me zitten. Tranen in de ogen, want ze werd uitgelachen op TikTok. Als bepaalde filmpjes openden, dan hoorde ze een keiharde lach door het filmpje heen, een beetje The Jokerachtig. Ze had verdriet om het lachje, want ze voelde zich uitgelachen. Ik heb dan altijd een beetje verdriet om haar tranen, maar ik voelde me eigenlijk ook uitgelachen, maar dan om een andere reden. Hier was duidelijk sprake van een indringer die in staat was door alle beveiligingen heen te hacken en die ons, met al onze goede beveiligingsbedoelingen, uit ging lachen. Dit was wederom een bewijs hoever men is op het gebied van indringing en hoe relatief eenvoudig het is.

Voorzitter. Spioneren, afluisteren, infiltreren, saboteren, het is van alle tijden, maar het neemt voortdurend andere vormen aan. Het vereist van ons dat we al het mogelijke doen om onze tegenstander telkens een stap voor te zijn. Waren we vroeger op zoek naar de man in de regenjas die op een regenachtige avond een geheime boodschap achterliet onder een bankje in het park, tegenwoordig vechten we tegen een veel minder zichtbare vijand die via digitale achterdeurtjes onze mobiele netwerken probeert binnen te dringen. Minder zichtbaar, maar niet minder schadelijk voor onze samenleving, burgers en bedrijven. Aanleiding voor dit debat was het bericht dat het Chinese Huawei in 2010 onbeperkt toegang had tot het netwerk van KPN. Een casus van weliswaar een aantal jaren geleden, maar nog steeds erg actueel. Het bedrijf is immers niet voor niets uitgesloten van de kritieke onderdelen van het 5G-netwerk. Tijdens het vragenuur op 20 april jongstleden gaf de staatssecretaris aan dat Agentschap Telecom onderzoek doet naar de KPN-casus. Is dit er al, en zo niet, wanneer komt het?

Centrale vraag tijdens dit debat: zijn onze mobiele netwerken, de kritieke onderdelen daarvan, op dit moment voldoende beschermd tegen buitenlandse, maar wat het CDA betreft ook binnenlandse spionage? Gelet op de vertrouwelijkheid van veel informatie zal een antwoord waarschijnlijk uitblijven, maar ik stip toch graag een aantal zaken aan die voor ons erg van belang zijn. Want de veiligheid voor onze mobiele netwerken heeft al heel lang de aandacht van het CDA. Zo blijkt uit de vele moties die mijn voorganger, mevrouw Van den Berg, op dit dossier heeft ingediend. Een motie die in het licht van dit debat cruciaal is, is de motie-Van den Berg/Bruins uit het wetgevingsoverleg over de Wet ongewenste zeggenschap telecommunicatie van 20 april 2020, die de regering verzoekt te bezien waar de sector na het aannemen van deze wet nog kwetsbaar is en of er aanvullende maatregelen nodig zijn. Hoe is er opvolging gegeven aan deze motie, vraag ik de staatssecretaris.

Bij het beschermen van burgers en bedrijven en het beveiligen van onze mobiele netwerken horen overheid en telecomproviders elkaars bondgenoten te zijn en goed samen te werken. Die laatsten moeten op dit moment fors investeren om een netwerk te beveiligen, onder andere door het verwijderen van onderdelen die aanvankelijk te goeder trouw gekocht zijn, maar nadien door de overheid verboden. Zij zouden aanspraak kunnen maken op nadeelcompensatie. Is dat zo? Wij ontvangen ook signalen dat de drempelwaarden uit het nadeelcompensatiekader dusdanig hoog zijn dat telecomproviders de facto niet voor nadeelcompensatie in aanmerking komen. Klopt dit, vragen wij de staatssecretaris.

Wanneer het gaat om het beveiligen van onze mobiele netwerken, ligt de focus vaak op de telecomnetwerken zelf, terwijl de rol van cyberveiligheid bij het gebruik van apps en mobiele toestellen veel minder aandacht krijgt. Eigenlijk ten onrechte, want als de Chinese app TikTok stiekem en op grote schaal informatie van kinderen kan verzamelen en verhandelen, dan moeten toch echt alle alarmbellen afgaan. Het CDA vindt dit zorgelijk en pleit voor nader onderzoek naar de kwetsbaarheden van appgebruik, zowel onder kinderen als onder volwassenen, en waar dit kan worden verbeterd. Graag een reactie.

Het laatste punt dat ik wil maken, en het is ook al eerder gezegd hier, is dat over strategische autonomie, of eigenlijk het gebrek daaraan. Nederland en Europa hebben zich in

de loop der jaren te afhankelijk gemaakt van Amerikaanse en Chinese technologie, waardoor het bedrijf Huawei ruim baan kon krijgen op onze markt. Voorwaar de reden dat het CDA pleit voor strategisch regionaal industriebeleid, waaronder reshoring, waarmee we onze afhankelijk van derde landen beperken. Welke stappen zet het kabinet op dit terrein? Graag een reactie.

De **voorzitter**:
Dank u. Mooi binnen de tijd. Dan geef ik het woord aan de heer Van der Lee van GroenLinks.

De heer **Van der Lee** (GroenLinks):
Dank u wel, voorzitter. Er zijn al heel veel vragen gesteld. Gemakshalve sluit ik me daarbij aan, ook bij de termijn van mevrouw Van Ginneken. Waarbij ik wel opmerk dat het rapport waar we het over hebben, al elf jaar oud is. Dat zijn bijna hondenjaren als het gaat om de telecom en nieuwe technologieën. Dat is eigenlijk al bijna 77 jaar geleden. Zo snel gaan die ontwikkelingen.

Ik moet ook zeggen dat ik in de jaren daarna ook weleens bij KPN ben geweest. In die periode hadden ze ook een topnotch cybersecurityteam. Dat behoorde tot de top drie in de wereld als het ging om het opsporen van mogelijkheden tot hacking. Er ligt dus een grote verantwoordelijkheid bij de bedrijven zelf, er moet veel meer aan gebeuren, maar er ligt ook een structureel probleem. En die structurele aanpak die ons is beloofd, komt niet van de grond. Dat geeft ook een van de providers aan. Ik vraag de staatssecretaris hoe dat komt.

Wat ik mij ook afvraag, is waarom wij — dat schept weinig vertrouwen — zo vertrouwelijk doen over deze informatie, daar waar andere landen veel opener zijn over wat bijvoorbeeld kritiek is. Die geven daar gewoon definities aan. Wat wil je per se niet geleverd hebben door een bedrijf als Huawei? Als je spreekt over de andere twee leveranciers, Ericsson en Nokia: die betrekken vrij veel van hun essentiële onderdelen ook weer uit China. Die afhankelijkheid is gewoon te groot. Daarom is het belangrijk dat wij werk maken van autonomie op dit terrein, meer diversificatie. Mijn fractie zou graag zien dat het kabinet ook onderzoek doet naar het stimuleren van open RAN-netwerken, waardoor het mogelijk is om van meerdere producenten producten te betrekken om dit soort zaken — ook 5G straks — in de toekomst van de grond te krijgen. Zo ver is het nog lang niet, maar wil je deze ontwikkelingen bij kunnen houden, dan moet je wat proactiever opereren als overheid dan nu gebeurt. Ik hoop dat de staatssecretaris daar stappen in wil zetten.

Als het gaat om dit soort ontwikkelingen, denk ik ook dat het belangrijk is dat we meer leren van de landen die hierin vooroplopen. Dat gaat om het Verenigd Koninkrijk met name. Gaan we daar langs? Vragen we aan hen hoe zij dit aanpakken? Leren we daarvan? Of proberen we allemaal weer opnieuw het wiel uit te vinden?

De Cyber Security Raad benadrukt dat het ook belangrijk is dat wij proactiever nadenken over hoe we kunnen bevorderen dat standaarden die wij belangrijk vinden — dan bedoel ik niet alleen in Nederland, maar in de Europese Unie — ook standaarden worden die mondiaal worden opgevolgd. Ook hier moeten we meer proactief handelen. Het gaat om gerichtere research and development, gerichtere overheidsstimulering en gerichtere telecomindustriepolitiek. Dat is een pleidooi dat mijn fractie al langer heeft gehouden. Wij hebben al jaren gewaarschuwd voor de rol van Huawei. We zien ook dat een eerder aangenomen motie die we met de VVD hebben ingediend over het in kaart brengen van afhankelijkheden vrij slecht wordt uitgevoerd. De toezegging is dan: de structurele aanpak die we in de telecom toepassen, gaan we verbreden. Maar er is nog helemaal geen structurele aanpak in de telecom. Ik heb weinig tastbaar bewijs dat we hier als overheid stappen in zetten. Ik benadruk wel dat ik vind dat het niet alleen aan de overheid is. Het is ook aan de marktpartijen, maar die hebben te maken met toenemende concurrentie. Die maken ook keuzes die niet per se onze veiligheid bevorderen. Als je dat echt wil, betekent dat dat daar consequenties aan vastzitten en dat je die als Nederlandse samenleving ook moet accepteren. Dat betekent dat je niet altijd voor de laagste prijs de beste technologie krijgt en dat je soms ook moet betalen voor de veiligheid en de privacy, die wij met elkaar hier in Nederland zo belangrijk vinden.

Ik wens de staatssecretaris veel succes met haar beantwoording. Ik hoop dat zij de Kamer ervan kan overtuigen dat die structurele aanpak echt vorm krijgt, dat zij ook gaat zorgen dat die wordt opgevolgd en dat er wordt onderzocht of die opvolging in de praktijk geïmplementeerd wordt. Ik hoop dat we daar rapportages over krijgen en dat we veel meer betrokken worden dan nu — dat geldt ook voor het publiek, want de burgers willen het ook weten — bij hoe het staat met onze telecom en de veiligheid daarvan en of onze privacy naar vermogen is geborgd.

Dank u wel.

De **voorzitter**:
Dank u. Dan geef ik tot slot het woord aan de heer Dassen van Volt.

De heer **Dassen** (Volt):
Dank, voorzitter. Dit debat gaat natuurlijk deels over de vraag hoe we op korte termijn spionage via buitenlandse techleveranciers kunnen voorkomen. Tegelijkertijd geeft de Wetenschappelijke Raad voor het Regeringsbeleid aan dat volledige digitale veiligheid niet bestaat en dat we het niet 100% kunnen voorkomen. Ik ben benieuwd hoe de staatssecretaris dat ziet.

Voorzitter. We kunnen wel stappen ondernemen om spionage via onze mobiele netwerken zo veel mogelijk te voorkomen, maar hier is ook een gezonde dosis realiteitszin nodig. Want het vervangen van buitenlandse techleveranciers door Europese techleveranciers maakt onze mobiele netwerken niet per definitie veilig. Veel Europese techbedrijven, waaronder Ericsson en Nokia, laten namelijk ook onderdelen van hun apparatuur in China produceren in samenwerking met Chinese staatsbedrijven. Als de Chinese overheid achterdeurtjes in onze mobiele netwerken wil bouwen, zou ze dat via deze route kunnen doen. Om de Europese autonomie te vergroten, zullen we de productie dus helemaal naar Europa moeten halen. Ik vraag me af of de staatssecretaris dat van plan is en, zo niet, wat dan de

risico's zijn en hoe we die mitigeren. Wie neemt hierin de voortrekkersrol?

Voorzitter. Het wordt ook tijd om de cruciale bedrijven voor de vierde industriële revolutie in de eerste plaats als Europese bedrijven te beschouwen in plaats van als Finse, Duitse of Zweedse bedrijven. Dit vergt ook een zekere inzet van Nederland. Ziet de staatssecretaris de noodzaak van een Europese industriepolitiek? Is de staatssecretaris ook bereid dit op Europees niveau uit te dragen? Momenteel lijken de VS de strategische noodzaak van deze bedrijven meer in te zien dan de Europese lidstaten. De VS hebben vorig jaar zelfs geprobeerd een meerderheidsbelang in Ericsson te verkrijgen, terwijl wij het in 2017 bijna failliet lieten gaan.

Voorzitter. Er is nog geen overzicht van wat de cruciale Europese bedrijven voor de vierde industriële revolutie zijn. Sterker nog, dat hebben we nog niet eens in kaart voor Nederland. Toen het drama rondom de hack bij DigiNotar zich in 2011 langzaam ontvouwde, wist niemand zeker hoe belangrijk dat bedrijf in Beverwijk was voor Nederland. Mijn vraag aan de staatssecretaris is wat zij er nu aan doet om een overzicht te verkrijgen van de meest cruciale Nederlandse techbedrijven in het kader van de cybersecurity. De EU is momenteel bezig met een inventarisatie op Europees niveau. Ik vraag mij af wat Nederland hieraan bijdraagt. Het is natuurlijk zaak om zo snel mogelijk een overzicht te krijgen, zodat we weten welke bedrijven we moeten beschermen tegen non-Europese overnames en concurrentie.

Tot slot moeten we kijken hoe we deze technologie slimmer gaan gebruiken. Welke informatie delen we met behulp van genetwerkte technologie en welke informatie zeker niet? We moeten ervoor zorgen dat elke organisatie consequent digitale kwetsbaarheden screent, patches en updates consequent uitvoert, en regelmatig back-ups maakt. Personeel moet uitvoerig getraind worden in cyberveiligheid. Dat is arbeidsintensief en vergt enorme investeringen. De 95 miljoen die de regering er de afgelopen regeerperiode voor uit heeft getrokken, is een schijntje in vergelijking met de 833 miljoen die de Cyber Security Raad minimaal nodig acht. Wat zijn de stappen die de staatssecretaris hierin neemt? Hoe wil zij, in navolging van wat de heer Van der Lee zei over het Verenigd Koninkrijk, hierbij leren van Estland? Daar zijn ze immers in korte tijd koploper geworden op het gebied van cyberveiligheid met een digitale overheid. Is de staatssecretaris met het oog op de toekomst nu al bereid om zich binnen de EU hard te maken voor een Europese 6G-strategie? Want het lijkt erop dat we niet de gewenste voortrekkersrol in 5G zullen hebben, maar wij kunnen het ons niet veroorloven om ook die boot te missen.

Dank u wel.

De **voorzitter**:
Dank u. Dan hebben we alle sprekers van de zijde van de Kamer gehad en schorsen we tot 19.40 uur, waarna de staatssecretaris de beantwoording zal doen.

De vergadering wordt van 19.21 uur tot 19.40 uur geschorst.

De **voorzitter**:
Ik geef het woord aan de staatssecretaris.

☐

Staatssecretaris **Keijzer**:
Dank u wel, voorzitter. We hebben het vandaag over de veiligheid en de integriteit van mobiele telecomnetwerken, en dan in relatie tot de risico's op spionage vanuit statelijke actoren. We hebben hier in het kader van het mondelinge vragenuurtje natuurlijk een debat gehad waarin een flink aantal van de vragen die vandaag voorbijkwamen ook aan de orde kwamen. Toen heb ik ook steeds gezegd: er zijn bepaalde dingen die ik gewoon niet in de openbaarheid met u kan delen, omdat ze de nationale veiligheid raken. Daar hebben we in dit huis een oplossing voor. Dan kunnen we namelijk een vertrouwelijke briefing houden. Op 18 mei is er zo'n briefing geweest om goed met u door te spreken wat nou de risico's zijn die we lopen, hoe dat in de praktijk dan gaat en wat kritieke onderdelen zijn. Dat is daar dus ook aan de orde geweest.

Wat ik in ieder geval van een flink aantal van u gehoord heb, is de zorg over dit soort activiteiten en over wat het betekent voor onze economie en onze samenleving. Daar zijn we het volgens mij met z'n allen over eens. Je moet echt je uiterste best doen om alles zo in te richten dat je de risico's zo goed als mogelijk beperkt. Het is namelijk in het belang van onze samenleving en onze economie dat je ervan kan uitgaan dat de mobiele telecommunicatienetwerken die je gebruikt, zo veilig mogelijk zijn. De heer Dassen was de laatste spreker en hij refereerde daar ook aan. Helemaal 100% veilig krijg je het nooit. Garanties zijn ook hier niet te geven, maar we doen wel alles wat in onze macht ligt om ervoor te zorgen dat het zo veilig mogelijk gaat.

Dat begint met de zorgplicht die opgenomen is in hoofdstuk 11a van de Telecommunicatiewet. Daarin is opgenomen dat aanbieders passende technische en organisatorische maatregelen moeten nemen om hun risico's te beheersen. Deze zorgplicht is in 2012 in de wet opgenomen. Hiermee ligt dus een grote eigen verantwoordelijkheid bij de aanbieders zelf. De heer Van der Lee refereerde daar terecht ook aan. Zij zijn ook verantwoordelijk voor de invulling daarvan. Zij hebben immers het beste zicht op hun systemen en zij kennen de risico's waarmee zij dagelijks te maken krijgen. Uit die zorgplicht vloeit voort dat aanbieders hun risico's en bijpassende maatregelen in een plan dienen vast te leggen. Het Agentschap Telecom houdt toezicht op die plannen. Het kijkt hoe die plannen eruit zien en als er onderzoek nodig is, dan kijkt het hoe dat vervolgens uitpakt. Een voorbeeld is het onderzoek dat het Agentschap Telecom op dit moment uitvoert naar aanleiding van het artikel in de Volkskrant dat ook de aanleiding was voor het debat tijdens het mondelinge vragenuur en waar ook vandaag weer aan gerefereerd wordt. Dat onderzoek is nog niet af. Ik moet de Kamer daar dus op een later moment over informeren. Ik ga dat ook doen.

Wat hebben we nou gedaan de afgelopen jaren? Welke acties heeft het kabinet al ondernomen en welke acties worden nog ondernomen om de risico's op spionage vanuit statelijke actoren bij mobiele netwerken tegen te gaan? Ik heb de Kamer op verzoek van mevrouw Van Ginneken op 15 juni een brief daarover gestuurd. Daarin heb ik ook weer niet alles kunnen zeggen. Dat heeft ermee te maken dat zaken nou eenmaal niet openbaar kunnen worden gedeeld als het bedrijfsvertrouwelijke informatie of de nationale veiligheid betreft. De geschetste maatregelen zijn mede op

basis van inlichtingeninformatie van onze diensten tot stand gekomen. Mede op basis daarvan is bijvoorbeeld ook bepaald welke onderdelen als kritiek zijn aangemerkt. Daarover doen wij vanuit het kabinet gewoon geen mededelingen in het openbaar. Dit kan namelijk zicht geven op het kennisniveau van de Nederlandse inlichtingen- en veiligheidsdiensten, en dat vinden wij ongewenst. Om u toch zo goed als mogelijk mee te nemen in die afweging — ik kan me voorstellen dat u dat gewoon wilt weten — hebben we dus die vertrouwelijke briefings.

Ons collectieve bewustzijn ten aanzien van de mogelijke kwetsbaarheid van mobiele telecommunicatienetwerken voor spionagerisico's vanuit statelijke actoren via leveranciers van technologie is de afgelopen jaren fors toegenomen. In de brief van 1 juli 2019 over het onderwerp maatregelen ter bescherming van telecomnetwerken en 5G hebben de AIVD en de MIVD vastgesteld dat infiltratie van dienstverleners door statelijke actoren spionage faciliteert.

De heer **Van der Lee** (GroenLinks):
Misschien ben ik te ongeduldig, maar de staatssecretaris vertelt dingen die we ook al via de stukken hebben mogen vernemen. Als ik weer dat verhaal hoor over wat er allemaal in vertrouwelijkheid moet, wil ik toch wel weten waarom de Britten dat anders doen. Zij hebben heel duidelijk gedefinieerd wat onbetrouwbaar is en wat kritiek is. Ze hebben een lange lijst met afkortingen van specifieke onderdelen van het netwerk gepubliceerd die specifieke aanbieders niet mogen aanleveren. Nemen zij dan hele grote risico's? Bieden zij dan inzage die wij niet kunnen bieden? Wat verklaart nou dat verschil?

Staatssecretaris **Keijzer**:
Dat is een vraag die u aan de Britse regering moet stellen. Er zijn ook landen die het niet doen. En daarbij, met het feit dat dit gepubliceerd is, weet je niet wat er niet gepubliceerd wordt. Elk land maakt daar een eigen afweging in. Dit is de afweging die het Nederlandse kabinet maakt. Omdat ik uw zorg goed begrijp, bieden wij ook technische briefings aan waarin u deze informatie wel allemaal kunt krijgen, waarin u door kunt vragen: wat is een kritiek onderdeel en wat niet, en waarom?

De heer **Van der Lee** (GroenLinks):
Ik ben in de gelukkige omstandigheid dat ik daar niet bij kon zijn, dus ik kan er ook geen geheimen uit verklappen. Dat was ik ook niet van plan, hoor, maar het gaat mij om de combinatie dat er landen zijn die transparanter zijn dan wij en dat wij tegelijkertijd van telecomproviders hier horen dat zij nog heel weinig merken van die structurele aanpak. Dan gebeuren er dus kennelijk dingen in beslotenheid waar niemand kennis van heeft, zelfs niet de doelgroep, namelijk de telecomproviders die hun veiligheid beter op orde zouden moeten krijgen. Dan denk ik dat wij als Kamerleden vanuit onze controlefunctie toch door moeten vragen en moeten aandringen op meer transparantie en duidelijkheid.

Staatssecretaris **Keijzer**:
Is er nou structueel overleg met de providers, zoals u aangetroffen heeft in die brief uit 2019? Jazeker. We hebben de afgelopen tijd natuurlijk uitgebreid met elkaar gesproken. Er is een algemene maatregel van bestuur gemaakt. Er is een ministeriële regeling, die inmiddels genotificeerd is in Brussel. Er zijn beschikkingen verstrekt aan providers. Zoals wij dat doen in dit land, doen wij dat in overleg met de providers. "Het structureel overleg", zoals dat genoemd wordt, waarin we aan het begin van de vergadering vaststellen "nou, in de brief van juni 2019 stond dat wij structureel overleg met u zouden hebben om te monitoren wat er aan de hand is, en dat doen we dan in één kamer met alle providers samen, de NCTV, het ministerie van EZK en het Nationaal Cyber Security Centrum" is er dus nog niet geweest. Maar dat komt doordat we in die tijd tussen februari 2020 en april 2021 constant met elkaar gesproken hebben over die algemene maatregel van bestuur, over de ministeriële regeling en over de beschikkingen die verstrekt zijn.

Mevrouw **Van Ginneken** (D66):
In tegenstelling tot de heer Van der Lee was ik wel in de gelegenheid om bij die technische briefing te zijn. De staatssecretaris geeft aan dat daar het nodige is gedeeld, maar ik vind dat ontoereikend. Het gaat er namelijk niet alleen om dat we de Kamer informeren, maar ook dat de samenleving geïnformeerd wordt over het grote risico dat er is in onze telecominfrastructuur. Ik denk dat ze daar recht op hebben. De staatssecretaris zegt steeds: er zijn dingen die ik niet kan delen in verband met de nationale veiligheid of bedrijfsvertrouwelijkheid. Maar ze maakt wat mij betreft niet aannemelijk dat bijvoorbeeld de datum waarop een brief is verstuurd naar telecomoperators, de datum waarop telecomoperators hun boel op orde moeten hebben, de nationale veiligheid zou bedreigen. Ik realiseer me dat de staatssecretaris nog een vervolg te gaan heeft in deze reactie, dus bij dezen de uitnodiging om die vragen zo meteen toch concreter te gaan beantwoorden.

Staatssecretaris **Keijzer**:
Daar waar ik openheid van zaken kan geven, doe ik dat. Maar ik hoop dat u begrijpt dat het juist in het belang van de Nederlandse burger is om informatie die nadelig is voor de nationale veiligheid niet te verstrekken. Dat is niet om geheimzinnig te willen doen, maar dat heeft ermee te maken dat je, als je zegt wat je wél weet, ook zegt wat je niet weet. En daar kan dan vervolgens weer misbruik van gemaakt worden. Ikzelf hou helemaal niet van onnodig geheimzinnig doen, dus daar kunt u bij mij ook op rekenen. Maar ik moet wel heel precies formuleren als het over dit soort zaken gaat.

Mevrouw **Leijten** (SP):
Het is nog maar anderhalf jaar geleden dat ik aan de staatssecretaris van Financiën voorstelde om de risicomodellen en de toegepaste algoritmes van Belastingdienst/Toeslagen eens openbaar te maken, zodat die getoetst konden worden op rechtmatigheid. Mij werd toen gezegd: nee, in het belang van de Staat kan dat niet! Het is een jaar geleden dat ze uit de lucht moesten worden gehaald omdat de Autoriteit Persoonsgegevens zei dat ze discriminerend waren. Nog altijd weten we overigens niet op welke punten dat was. Het gaat mij erom dat het niet aan de staatssecretaris is om te zeggen wat er niet gedeeld kan worden met de Kamer in het belang van de Staat. Hoe wil ze dat gaan oplossen?

Staatssecretaris **Keijzer**:
Er is een technische briefing geweest, waarbij ook de fractie van de SP niet aanwezig was. Daarmee wil ik niet zeggen dat de fractie van de SP het niet belangrijk vindt, want ik weet hoe druk de agenda's zijn. Dat is waarom ik ook nu weer aanbied om alsnog zo'n technische briefing te houden, waarbij u aanwezig kunt zijn en u alle vragen kunt stellen. In zo'n vertrouwelijke briefing kunt u dan antwoord op uw vragen krijgen. Maar ik kan het hier gewoon niet delen, overigens ook omdat het niet direct mijn verantwoordelijkheid is. Daarvoor moet u met de verantwoordelijke bewindspersonen het debat aangaan. Het is niet aan mij om hier dingen te zeggen waarvan wij in het kabinet hebben vastgesteld dat ze onder de nationale veiligheid vallen.

De **voorzitter**:
Dank. Ik zie mevrouw Leijten voor een tweede interruptie.

Mevrouw **Leijten** (SP):
Deze staatssecretaris heeft heel veel ervaring met vertrouwelijke briefings en hoe je daarmee gemuilkorfd wordt. Er is zelfs nog een interessant boek geschreven over hoe dat onze rechtsstaat raakt. Dat boek heet Een sociaal contract. Volgens mij moeten we hier zo veel mogelijk van af. Ik stelde nou juist de vraag hoe we samen kunnen bepalen wat er wel en niet naar buiten kan komen, omdat we afscheid moeten nemen van de cultuur van "wat we niet willen delen, maken we vertrouwelijk en dat doen we in een vertrouwelijke technische briefing, en we leggen de Kamerleden aan de ketting". Ik zou het zo mooi vinden als deze staatssecretaris er eens over na wil gaan denken hoe zij samen met de Kamer, desnoods met onafhankelijke experts erbij, kan kijken of het daadwerkelijk nodig is dat dit vertrouwelijk blijft, juist ook door de vraag die de heer Van der Lee stelde over andere landen, die er anders mee omgaan, en juist omdat wij allemaal gevraagd hebben, dus alle fracties die deelnemen, of u ons wat meer kunt vertellen over de strategische keuzes die gemaakt worden. Het is niet meer goed genoeg om dat allemaal vertrouwelijk te verklaren.

Staatssecretaris **Keijzer**:
Je hebt natuurlijk vraagstukken die gaan over beleidsafwegingen, en vraagstukken die raken aan de nationale veiligheid. En je hebt vraagstukken waarbij bedrijfsvertrouwelijke informatie betrokken is. Bedrijfsvertrouwelijkheid is ook een van de gronden waarop je geen informatie mag verstrekken. Daar zijn bedrijven bij betrokken, die dan gewoon hun vinger opsteken en zeggen: dat is mijn eigendom; dat mag u niet delen. Of: als u dat deelt, benadeelt dat mijn positie. Ik ben dus zeer bereid om hierover in gesprek te gaan met de Kamer. We hebben nog anderhalve week Kamerdebatten. Ik ben zeer bereid om desnoods in de eerste week van het reces, als hopelijk iedereen kan, nogmaals een technische briefing te organiseren, waarbij u dan allemaal aanwezig kunt zijn. Ik ben zeer bereid om met de griffie te kijken naar een moment waarop we dat kunnen organiseren. En dan krijgt u al die informatie. U mag het wel, maar ik kan u nu geen informatie verschaffen waarvan wij in het kabinet hebben vastgesteld dat het de nationale veiligheid raakt.

Mevrouw **Leijten** (SP):
En daarmee praten we dus over lucht. Dat is zo erg. De Kamerleden die het wel weten, mogen het niet zeggen. Want dan wordt daar meteen van gezegd dat ze lekken of dat ze zich niet aan de regels houden, terwijl wij ook niet kunnen zeggen: ho, maar wacht eens even, daar zijn dingen besproken waarvan we gewoon willen dat ze openbaar zijn. Ik zou het nou juist zo waardevol vinden als deze staatssecretaris toch een beetje de randen gaat opzoeken. Niemand zit hier te wachten op informatie die onze positie als Nederlandse Staat of onze Nederlandse bedrijven zou bedreigen. Niemand vraagt daarom. We vragen wel om de informatie waardoor wij kunnen toetsen, ook met onafhankelijke derden, journalisten en met wetenschappers die meekijken, of we de juiste keuzes maken. Daar gaat het hier om. Dat weet mevrouw Keijzer heel erg goed. Zij is een heel ervaren Kamerlid en een heel ervaren staatssecretaris. Probeer nou eens langs die lijn te denken, want we staan hier te veel over lucht te praten. Dat is volgens mij minder nodig dan wordt voorgesteld.

Staatssecretaris **Keijzer**:
We staan hier niet over lucht te praten. We staan hier met elkaar te praten over de maatregelen die het kabinet genomen heeft om te werken aan de integriteit en veiligheid van onze telecommunicatienetwerken. In de brief van juni 2019 kunt u daar veel over lezen. In de brief van 15 juni 2021, in antwoord op vragen van mevrouw Van Ginneken, kunt u daar het een en ander over lezen. Nogmaals, ik ben meer dan bereid om nogmaals een technische briefing te houden. Dan gaan we met elkaar op zoek naar een datum waarop u allemaal kan. Want ik weet hoe drukbezet u bent. Ik denk dat het goed is dat u ook met uw fractievoorzitters over dit onderwerp spreekt. Want die zitten nog met elkaar … Ik vergeet altijd de officiële afkorting. Het is nooit zo netjes om commissie-stiekem te zeggen. Maar dat is de CIVD, volgens mij. Ja, hè? Die. Nou, daarin zitten de fractievoorzitters in vertrouwelijkheid bij elkaar om te spreken over nationale veiligheid en daaraan gelieerde onderwerpen. Het is gewoon niet aan mij om hier nu meer over te zeggen dan wat wij daarover hebben vastgesteld in het kabinet, zijnde datgene wat niet raakt aan de nationale veiligheid.

De **voorzitter**:
Ik wilde eigenlijk zeggen: gaat u door naar het volgende punt. Maar ik zie toch nog een interruptie van mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Het volgende punt ben ik dan heel even. Ik vind dit toch onvoldoende. Ik vind dat de staatssecretaris al onze kritische vragen een beetje toedekt met op het oog warm klinkende toezeggingen om ons nog een keer in een vertrouwelijke sessie te briefen. Maar de essentie van waar het hier over gaat laat ze onbeantwoord, namelijk dat de samenleving vertrouwen moet hebben, houden en krijgen in onze mobiele telecominfrastructuur, en dat dat vraagt dat bedrijven, wetenschappers en techexperts mee kunnen kijken met wat hier gebeurt. Nogmaals, heel veel van wat vertrouwelijk gedeeld is, is niet aan mij om aan de samenleving uit te leggen. Ik hoop dat de staatssecretaris de samenleving niet langer laat bungelen en meer haar best doet om dingen openbaar te maken.

De **voorzitter**:
Dank. De staatssecretaris is nog niet klaar met haar verhaal. Ik geef haar het woord om verder te gaan.

Staatssecretaris **Keijzer**:
Nee, voorzitter, nog lang niet. Ik maak toch een beetje bezwaar tegen de woorden van de vertegenwoordiger van de fractie van D66. Want het is niet zo dat wij de samenleving overlaten aan spionage. Honderd procent garanderen dat het niet meer gebeurt, kan ik niet. De heer Dassen zei dat terecht. Maar we zijn heel concreet bezig geweest met wat we dan wel kunnen doen om maatregelen te treffen. En dat is een boel. Mobiele netwerkaanbieders worden verplicht om aanvullende technische en organisatorische beveiligingsmaatregelen te nemen, bijvoorbeeld specifieke eisen aan toegang tot telecomsystemen door derden. Deze eisen zijn opgenomen in een ministeriële regeling. Die wordt inmiddels genotificeerd bij de Europese Commissie. De verwachting is dat die eind september in werking treedt. Gaan providers dan pas daarmee aan het werk? Nee, natuurlijk niet, voorzitter. Die zijn niet gek. Die hebben een zorgplicht op basis van de Telecomwet sinds 2012. Bij hun investeringsbeslissingen houden ze natuurlijk rekening met de eisen waarvan ze weten dat die vanuit het kabinet zullen komen.

Ze zijn onlangs verplicht om in de kritieke onderdelen van hun netwerken voor producten en diensten uitsluitend gebruik te maken van andere partijen dan de in de beschikking genoemde leveranciers. En ja, het heeft wel een tijd gekost om die vast te stellen, zeg ik tegen mevrouw Van Ginneken. Maar ook hiervoor geldt: toen die verstuurd werden, hoorden ze dat natuurlijk niet voor het eerst. Dit is onderdeel van het gesprek, het structureel overleg zoals ik net tegen de heer Van der Lee zei. Ze zouden natuurlijk wel gek zijn om nog in zee te gaan met het bedrijf dat niet valt onder de lijst die wij hebben vastgesteld met elkaar. Daarnaast wordt deze werkwijze ... Cybersecurity is niet iets waarvan je zegt: we hebben dit, dat en dat gedaan, dus nu zijn we klaar. Zeker gezien de technologische ontwikkelingen gaat dat over elke keer kijken wat voor informatie de diensten krijgen en wat voor consequenties we daaraan moeten verbinden. Die werkwijze is in de Taskforce Economische Veiligheid bestendigd en wordt in een structureel proces natuurlijk ook gewoon zo uitgevoerd. Zo blijven we adaptief op nieuwe ontwikkelingen, waarbij elke keer weer risicobeoordelingen worden uitgevoerd.

Voorzitter. Het CDA vroeg in een aantal moties van mevrouw Van den Berg om hen te betrekken bij de stappen. Dat zijn ze dus ook. Deze moties riepen ook op tot een Europees gecoördineerde aanpak van de integriteit van 5G-netwerken en om conform de Europese aanpak ook niet-technische kwetsbaarheden, zoals invloeden van staten op leveranciers, mee te nemen in de risicoanalyse. Ik heb destijds, in december 2019, in de Telecomraad actief gepleit voor een Europees gecoördineerde aanpak. Dat was toen nog niet een vanzelfsprekendheid, maar dat hebben we als Nederland gered. Het heeft geleid tot een toolbox die vastgesteld is op Europees niveau. In de geopolitieke context waarin dit vraagstuk speelt, onderschrijf ik dan ook het belang om Europees met elkaar op te trekken en af te stemmen waar het kan. De toolbox bevat zowel technische maatregelen als niet-technische maatregelen, zoals het uitsluiten van hoogrisicoleveranciers. De maatregelen die Nederland genomen heeft, zijn in lijn met die toolbox. De technische eisen staan in de ministeriële regeling.

Voorzitter. Alles bij elkaar opgeteld, doen we dus in ieder geval wat mij betreft al het mogelijke wat we kunnen, op basis van de informatie die we nu hebben. We hebben een structurele aanpak om elke keer weer te kijken: zijn we nog up-to-date? Is er wellicht nog meer nodig? Zo ja, wat dan?

Voorzitter. Het onderzoek van Agentschap Telecom naar de inbreuk in 2010 bij KPN wordt verwacht. Wij verwachten dat het eind september 2021 klaar is. Uiteraard zal ik u daarover informeren.

De **voorzitter**:
U heeft een interruptie op dit punt van de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Dank aan de staatssecretaris. Ik heb nog even een vraag. Behelst de zorgplicht ook de plicht voor iedere provider om, zodra hij iets ontdekt wat een risico is, dat ook proactief bij de toezichthouder te melden?

Staatssecretaris **Keijzer**:
Dat weet ik niet heel precies, omdat de vraag hierbij dan ook weer is: wat is dan een inbreuk? Is die heel groot, of heel klein? Kun je er meteen op acteren? Ik kom graag in tweede termijn terug op die vraag, om te kijken of ik daar wat meer duiding aan kan geven.

Voorzitter. Dan kom ik op de vragen die aan mij gesteld zijn. De vraag van de fractie van D66. Mevrouw Van Ginneken had het over vijftien maanden, maar het is langer geleden dat we de beschikkingen verstuurd hebben. Zoals ik net ook al aangaf, heeft het tijd nodig gehad om met elkaar te kunnen vaststellen wat er nodig is, maar ook om vervangingstermijnen te bepalen. Hierbij heb je een balans nodig tussen zo snel mogelijk vervangen vanwege de nationale veiligheid en een haalbare termijn vaststellen om de continuïteit van de dienstverlening in stand te houden. Plat gezegd: telecommunicatie moet natuurlijk wel door kunnen gaan en niet uit de lucht vallen. Met de gekozen termijnen wordt mijns inziens de balans gevonden. De termijnen zijn weer aan u bekend gemaakt in de technische briefing.

Mevrouw **Van Ginneken** (D66):
Voor mij is dit weer zo'n voorbeeld van het net niet helemaal goed kunnen vastpakken. Ik hoor de staatssecretaris zeggen dat de beschikkingen langer geleden verstuurd zijn. Tegelijkertijd heeft de staatssecretaris als reactie op het artikel in de Volkskrant halverwege april aangegeven dat op dat moment de beschikkingen nog niet verstuurd waren. In het commissiedebat heeft ze aangegeven dat ze kort daarvoor verstuurd waren, dus ergens tussen — laten we zeggen — 18 april en 18 mei zijn ze verstuurd. Als ik tel vanaf december 2019, kom ik toch op ruim vijftien maanden. Dus ik begrijp niet zo goed met welke termijn de staatssecretaris nu precies rekent. Ik zou heel graag een concrete datum horen waarop die beschikkingen verstuurd zijn.

Staatssecretaris **Keijzer**:
Ik rekende vanaf juni 2019 en dan heb je wat meer dan vijftien maanden. Ik heb u uiteengezet wat de redenen daarvoor zijn. Ik heb u ook uiteengezet dat dit niet betekent dat ze pas maatregelen hebben genomen op het moment dat de beschikkingen op de mat vielen. Het zijn natuurlijk verantwoordelijke bedrijven. Ze zijn niet gek. Ik heb de datum van verzending hier niet paraat, maar ik vind het ook wel van belang om te weten waarom ... Nou ja, "waarom" klinkt zo beschuldigend; zo bedoel ik het niet. Maar wat is de reden dat mevrouw Van Ginneken dat wil weten? Want als ik dat weet, kan ik ook kijken of ik wat met de vraag kan.

Mevrouw **Van Ginneken** (D66):
Die vraag beantwoord ik heel graag. Ik wil dat weten om te kunnen vaststellen of de staatssecretaris in die periode voldoende tempo heeft gemaakt met het oplossen van het probleem. Zoals ik net al zei, ervaar ik een gat in het cv als ik de brief lees die de staatssecretaris 15 juni aan de Kamer heeft gestuurd. Nou realiseer ik mij dat dit geen sollicitatie is, maar doorgaans wil je zo'n gat verklaard zien. Daar ben ik dus naar op zoek. Ik denk dat we daar met z'n allen behoefte aan hebben.

Staatssecretaris **Keijzer**:
Nu snap ik het gat in het cv. Het klopt. Het heeft zeker vijftien maanden geduurd. De precieze datum heb ik hier niet paraat, maar nogmaals, dat is absoluut geen gat in het cv. Want in die tijd is geprobeerd om Europa op één lijn te krijgen; daar is aan gewerkt. Dat heb ik u net verteld. Er is een algemene maatregel van bestuur gemaakt en vastgesteld. Er is gewerkt aan een ministeriële regeling. Er is in een gesprek met de providers vastgesteld waar nou de kritieke onderdelen zitten en waar maatregelen moeten worden genomen. We hebben het gehad over vervangingstermijnen. In die tijd is dus echt keihard gewerkt aan de veiligheid en integriteit. Tussen de termijn van de brief van juni 2019 en de beschikkingen zit inderdaad anderhalf jaar, maar dat wil niet zeggen dat je in die tijd niets gedaan hebt, integendeel. Ik heb net uiteengezet wat er allemaal gebeurd is.

De **voorzitter**:
Tot slot, mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Ik geloof dat ik de zoektocht naar een concrete datum hier even staak. Ik heb er alle begrip voor dat de staatssecretaris de exacte datum niet paraat heeft. Het ging mij erom dat ik hele aanloop naar waar we vandaag staan, helder wilde krijgen. Het is nog niet helemaal helder geworden, maar belangrijker is hoe het probleem opgelost gaat worden. Ik hoop dat de staatssecretaris daarop zo meteen wel heel specifiek en concreet kan ingaan.

Staatssecretaris **Keijzer**:
De beschikkingen zijn verstuurd. De vervangingstermijnen zijn met u gedeeld in een vertrouwelijke briefing. Eigenlijk heb ik op dit moment niet veel meer informatie dan dat. Daarmee heb ik wat mij betreft aangetoond dat we echt heel consequent aan het werken zijn aan de integriteit van die netwerken.

Voorzitter. Dan kom ik bij de vraag van de VVD-fractie: worden mensen en systemen gecontroleerd wanneer zij werken aan kritische delen van de vitale infrastructuur? Dat is een van de eisen die zijn opgenomen in de ministeriële regeling, die ik in de brief van 15 juni 2021 ook noem: mensen die werken aan kritische delen van de telecominfrastructuur moeten een achtergrondonderzoek krijgen. Hiervoor geldt natuurlijk ook dat een zichzelf serieus nemende provider niet wacht op het vaststellen van die ministeriële regeling; hij heeft namelijk een zorgplicht. Nogmaals, ze zouden wel gek zijn om het risico te lopen dat daar op een gegeven moment iets misgaat, want dan moeten zij uitleggen waarom ze gewacht hebben op die datum. Dat doe je natuurlijk niet. Ook daar wordt de integriteit van de netwerken buitengewoon serieus genomen.

Even kijken. Deze vragen heb ik ook allemaal al beantwoord in mijn beantwoording tot nu toe. Dan mevrouw Kathmann, die mij vroeg of het niet gewoon beter is om bepaalde bedrijven helemaal te weren. Wij hebben een risicogestuurde aanpak. Wij gaan uit van actuele dreigingen, daadwerkelijke informatie vanuit de diensten en te beschermen belangen en kijken dan met welke maatregelen risico's kunnen worden aangepakt. Dit heeft dus geleid tot beschikkingen en ministeriële regelingen. Het is een structurele aanpak en we blijven doen wat nodig is. Het is ook enigszins schijnveiligheid om te zeggen: nou, deze bedrijven niet meer en dan zijn we veilig. Zo werkt het gewoon niet, want dan komt er vervolgens een ander bedrijf of een andere statelijke actor die foute dingen wil. Wat mij betreft is het dus juist heel goed dat we het op deze manier hebben ingezet.

Voorzitter. Mij werd door de fractie van het CDA gevraagd naar de nadeelcompensatie. Voor het vergoeden van nadeel van op zichzelf rechtmatige overheidsbesluiten geldt het leerstuk van nadeelcompensatierechten. Het uitgangspunt is dat eenieder die nadeel lijdt vanwege zo'n rechtmatig uitgevoerde bevoegdheid of publieke taak, dit nadeel in beginsel zelf dient te dragen. Alleen onevenredige schade die het normale ondernemersrisico overstijgt, wordt vergoed. Dit is steeds de lijn van EZK geweest en zo zit ook dat leerstuk van nadeelcompensatie in elkaar. De drempel wordt bepaald aan de hand van een bepaald percentage van de omzet of kosten van de onderneming. Het is dus geen absoluut bedrag. Vanwege de bijzonderheid van de maatregelen heb ik de drempelwaarden voor onevenredige kosten aanmerkelijk lager gelegd dan in andere nadeelcompensatietrajecten. Voor zover de kosten deze drempel overstijgen, zullen deze als nadeelcompensatie worden vergoed. Voor de rest geldt hiervoor dat dit soort besluiten van de overheid uiteindelijk ook getoetst kunnen worden bij de rechter.

Voorzitter. Dan kom ik bij mijn volgende mapje. Ik ga even bezien of ik deze vragen ook al heb beantwoord in het eerdere verhaal. Ja, voorzitter, dat heb ik. Dit betreft een vraag van mevrouw Rajkowski. In de gesprekken die wij hebben met bedrijven, diensten, de NCTV en andere betrokkenen komt het elke keer weer terug op dat structurele proces.

Voorzitter. Dan het vraagstuk van digitale autonomie. Dit is een debat dat gaat over spionage in mobiele telecommu-

nicatienetwerken. Ik zal mij gezien de orde van deze vergadering dus een beetje beperken, maar ik wil daar wel een aantal dingen over zeggen. Wij zijn een open economie, waar in principe iedereen welkom is om handel te drijven. Alleen zijn we binnen Europees verband zo langzamerhand wel tot de conclusie gekomen dat dat dan wel is op onze voorwaarden. Dat is waarom bijvoorbeeld — een compleet zijstapje —- door Timmermans in de Green Deal is opgenomen dat als je eisen gaat opleggen aan je eigen bedrijfsleven vanwege duurzaamheid, je die ook moet opleggen aan bedrijven van buiten de Europese Unie. Dat betekent ook dat je in aanbestedingen wel moet gaan opletten dat bedrijven uit derde landen die worden gesubsidieerd door de overheid, niet ver onder de prijs van Europese bedrijven kunnen komen. Dat betekent ook dat in de Wet ongewenste zeggenschap telecom, die inmiddels door beide Kamers heen is, is opgenomen dat niet alle fusies en overnames in de telecomsector acceptabel zijn. Dat betekent ook … Daarover is eerder vandaag een debat geweest, waarin de heer Amhaouch een motie indiende om toch goed te kijken of Nederland aangehaakt kan blijven bij de Important Projects of Common European Interest en dan vooral de projecten die zien op de cloud en op micro-elektronica, bijvoorbeeld chips.

Wij zijn een open economie. Dat heeft ons veel gebracht, maar we zijn inmiddels wel wat stappen aan het zetten om toch eens preciezer te kijken of we niet te afhankelijk van anderen zijn en of we niet te makkelijk bedrijven hier toelaten op onze eigen markten terwijl die niet hebben te voldoen aan eisen en voorwaarden waar Europese bedrijven wel aan hebben te voldoen? Dit is wel een balans. Je moet goed nadenken waar je de grens legt. De heer Van der Lee sprak daarover. Europese bedrijven maken gebruik van onderdelen uit derde landen. Als we zeggen "we gooien de poorten dicht en dan komt alles goed", zou het zomaar eens kunnen zijn dat essentiële onderdelen hier niet meer binnenkomen. Daarnaast is het in een geopolitieke context goed om toch ook een klein beetje afhankelijk van elkaar te blijven. Dat houdt de boel soms ook netjes. Niet altijd, maar het helpt wel. Daarmee heb ik wat mij betreft ook deze vragen beantwoord.

Voorzitter. Mevrouw Leijten hield een betoog dat ik erken en herken als een echt SP-betoog. Zij vroeg mij of ik niet eens een visie zou moeten vormen op juist de vraag die wegkomt achter deze discussie: zouden bepaalde taken niet weer des overheid moeten worden? Een zeer interessant debat, maar ik ben een demissionair staatssecretaris, dus het is niet aan mij.

De **voorzitter**:
U hebt wel een vraag van de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Ik ben het eens met de staatssecretaris dat het niet zwartwit is. Een simpele oplossing bestaat niet, maar het besef dat we meer moeten diversifiëren is er inmiddels echt al een aantal jaren. Wat uitblijft, zijn hele duidelijke en concrete stappen naar een veel actievere industriepolitiek die niet alleen technologieneutraal is, maar waarin ook keuzes worden gemaakt. Je moet als overheid niet alles oplossen, maar je moet er wel voor zorgen dat er in de brede Europese Unie nieuwe bedrijven ontstaan die die concurrentie aankunnen. Wat mij verbaast, is dat Nederland, als het erop aankomt, eerder voor het belang van de open economie en de handel kiest dan voor het maken van die inhoudelijke keuzes. De staatssecretaris gaat dan weer zeggen "ik ben demissionair", maar toen het kabinet missionair was, heb ik deze kritiek ook al geuit en werden die keuzes ook niet gemaakt. Ik hoop dat de staatssecretaris in haar denken al verder is en dat zij met mij hoopt dat het nieuwe kabinet wél meer keuzes gaat maken. Dat is noodzakelijk. Anders komen we in deze discussie niet verder.

De **voorzitter**:
Nou staatssecretaris, antwoord op deze vraag.

Staatssecretaris **Keijzer**:
Dank u wel, voorzitter. Dat is ook buiten de orde, maar in het innovatie- en topsectorenbeleid maken wij natuurlijk keuzes. Dat doen wij. In het kader van het Nationaal Groenfonds worden ook keuzes gemaakt. We investeren in belangrijke onderwerpen en in belangrijke technologieën —"bedrijfstakken" is het verkeerde woord — die het verdienvermogen van Nederland in de toekomst kunnen gaan bepalen. Ik ben een demissionair staatssecretaris, maar ik was op zichzelf blij met de motie waar ik het net over had, als die tenminste aangenomen wordt. Daaruit zou namelijk blijken dat ook de Kamer de ontwikkeling op die IPCEI's cloud en micro-elektronica ziet. Ik kan nu alleen geen stappen zetten die nieuw beleid betekenen of nieuw geld vragen. Dat is dan maar het lot van een demissionair staatssecretaris, die best wel meningen heeft, maar dat weet u ook.

De **voorzitter**:
Ik zie de heer Dassen naar de microfoon lopen voor een interruptie.

De heer **Dassen** (Volt):
Ik heb een vraag over Europese bedrijven die ook in China produceren en vaak ook met Chinese staatsbedrijven. De staatssecretaris zegt: we zijn een open economie, we drijven handel en hier hebben we mee om te gaan. Mijn vraag is echter: wat zijn de risico's die u daar ziet? Wat zijn de mitigerende acties? Wie heeft daar de voortrekkersrol in? Kortom, worden een strategie en een visie gevormd voor hoe we daar in de toekomst mee omgaan?

Staatssecretaris **Keijzer**:
Ja. Wij hebben een brief verstuurd — volgens mij eind vorig jaar — over de maakindustrie. Daar gaan we nu een actieagenda op maken, om ook daar weer te kijken wat je hier kunt doen om te voorkomen dat je afhankelijk wordt op essentiële onderdelen. In die zin hebben we natuurlijk ook wel van de coronacrisis geleerd, toen we op een gegeven moment tot de conclusie kwamen dat we hier behoefte hadden aan beschermingsmiddelen, alleen werden die hier niet meer gemaakt. Ik weet niet of de heer Dassen dat bedoelt, maar zijn vraag was best algemeen.

De heer **Dassen** (Volt):
De vraag was specifiek bedoeld voor telecomnetwerken en de onderdelen die daarvoor gemaakt worden, deels ook door Europese bedrijven in China.

Staatssecretaris **Keijzer**:
Ik begrijp niet waar de heer Dassen …

De **voorzitter**:
Meneer Dassen, wilt u het nog een keer formuleren? Misschien komen we er dan uit.

De heer **Dassen** (Volt):
Een gedeelte van het netwerk of onderdelen daarvan worden gemaakt in China. Dat gebeurt door Europese bedrijven daar, maar vaak met Chinese staatsbedrijven. Mijn vraag aan de staatssecretaris is of zij daarvan risico's ziet en hoe die risico's worden gemitigeerd, specifiek op dat netwerk, dus voor de telecom.

Staatssecretaris **Keijzer**:
Dat is waarom ik sprak over de IPCEI-cloud en micro-elektronica, wat je ook zou kunnen vertalen als chips. Dat zijn de vraagstukken van de toekomst. Hoe zorg je dat je op die belangrijke onderdelen van onze digitale samenleving ook zelf iets kunt en zelf ook van betekenis bent? ASML en XP zijn twee grote spelers die van wereldbetekenis zijn, deels gevestigd in Nederland en daar ben ik blij mee. Bij ASML worden chipmachines gemaakt en dat bedrijf is gegroeid omdat we ooit een keer geïnvesteerd hebben in Philips, dat dreigde om te vallen. Dat is af en toe het gevoel dat mij bekruipt als ik naar die IPCEI-discussie kijk. Hoe zorgen we er nu voor dat we niet — een vreselijk idee — de volgende ASML buiten Europa hebben zitten en die producten hier zelf helemaal niet meer maken? Dan ben ik nog wel patriot genoeg om te kijken of we het een beetje hier in Nederland kunnen houden. Dat is ook goed voor de werkgelegenheid en voor de economische groei. In zijn algemeenheid zie ik wat de heer Dassen schetst en zijn we ook op onderdelen aan het kijken wat we daarin kunnen. IPCEI's zijn daar een voorbeeld van.

De **voorzitter**:
Een interruptie van mevrouw Kathmann.

Mevrouw **Kathmann** (PvdA):
Ik borduur even voort op dat pareltje van een vraag van de heer Dassen, dus alle credits naar hem. Dit zet mij wel aan het denken. Wat de heer Dassen volgens mij bedoelt, is: we hebben nu geïnventariseerd wat de vitale delen van onze digitale infrastructuur zijn. Op bepaalde vitale delen willen we geen inmenging van derde landen en bepaalde techbedrijven. Daar hebben we dan een lijstje voor. Dat is de Europese toolbox. Maar dat is ook weer een beetje schijnveiligheid, omdat de meeste Europese producenten hun fabrieken in Shenzhen hebben staan en daar werken ze vaak ook nog eens samen met die Chinese techbedrijven. Hoe gaan we hiermee om? Zolang de digitale maakindustrie op die vitale delen niet in Europa ís, maar in China, hebben wij geconstateerd dat we die inmenging niet willen op die vitale delen. Daarom zeggen we: die andere producenten mogen dat niet, maar eigenlijk doen de Europese producenten hetzelfde, want die maken het in China. Hoe gaan we met dat gevaar om? Hebben we daar en plan op, Europees dan wel nationaal?

Staatssecretaris **Keijzer**:
Hiervoor is niet de oplossing om alles wat wij gebruiken, in Nederland of misschien zelfs in Europa te maken. Dit zijn internationale productieketens waar onderlinge afhankelijkheid bestaat. Zoals gezegd is dat niet altijd slecht. Dat is de ene kant van deze discussie. De andere kant van deze discussie is: hoe zorg je dat je in Europa — ik ben een Nederlandse staatssecretaris — en in Nederland ook bepaalde productiecapaciteit en faciliteiten houdt? Dat is een proces waar je constant naar op zoek bent, waarbij je ook afhankelijk bent van bedrijfsleven en bijvoorbeeld vestigingsklimaat, wil het bedrijfsleven hier ook blijven. Dat is die kant daarvan. Vervolgens hebben we natuurlijk de risicogestuurde aanpak in het kader van de Taskforce Economische Veiligheid, waar ik aan het begin van dit debat het een en ander over verteld heb. Die is namelijk dat we elke keer op basis van informatie en inlichtingen van de diensten samen met bedrijven kijken welke risico's zij zien en eventueel komen tot nieuwe noodzakelijke maatregelen.

Mevrouw **Kathmann** (PvdA):
Ik heb nog één vraag, want ik vind dat een fijn antwoord, maar nog niet helemaal. De vraag is dan wel: kennen we die bedreigingen voldoende en wat zijn die? Want in de brieven die u heeft gestuurd en in alles wat aan de tafels besproken is, ook met de telecompartijen, is er heel bovengekomen en ook heel veel gedefinieerd, maar de bedreiging eigenlijk niet. De productie is wel in China, maar aan de andere kant willen we dat niet. Maar het is wel gewoon een feit. Wat zijn dan die bedreigingen door het feit dat die fabrieken daar staan? Hoe zorgen we dat die fabrieken veilig zijn en dat de productie veilig is? Ik zou nog wel een inventarisatie willen op het veiligheidsvraagstuk dat we nu hebben zolang heel veel maakindustrie niet in Europa is.

Staatssecretaris **Keijzer**:
Deze vraag komt bij mij binnen — ik maak hem even plat; excuses daarvoor — als: wil de regering in fabrieken in derde landen gaan controleren hoe daar de hardware in elkaar gezet wordt? Dat kan niet. Wat wij wel kunnen doen, en dat is wat de diensten doen, is goed in de gaten houden welke risico's we lopen en welke spionageactiviteiten er zijn. We hebben het erover gehad of ik die met u kan delen, maar daar wordt elke dag naar gekeken. Daarover gaat het in die structurele aanpak in gesprek met de NCTV, het Nationaal Cyber Security Centrum, EZK en de providers.

De **voorzitter**:
Dit roept nog een vraag op bij mevrouw Van Dijk.

Mevrouw **Inge van Dijk** (CDA):
In aanvulling daarop: op het moment dat er delen in die landen geproduceerd worden, weten we dat dan überhaupt? Weten we überhaupt waar onderdelen vandaan komen?

Want we kunnen van alles aan beveiliging inrichten, maar als we niet weten waar de onderdelen vandaan komen, is dat ook een beetje een laffe maatregel.

Staatssecretaris **Keijzer**:
Ja, en toch. Ik heb hier een — je mag zo wel namen noemen, hè? — iPhone liggen. Er zijn vast mensen onder u die een Samsung hebben of een Ericsson. Weet u allemaal precies ... Sorry? Een Huawei? O, hemel. Weet u allemaal precies wat daar allemaal in zit en waar dat vandaan komt? Nee, dat weet u niet. Daarnaast moet er ook verschil gemaakt worden. In de inbreng van mevrouw Van Dijk ging het over Jip, als ik het goed gehoord heb. Ja, daar krijg je kippenvel van. Daar krijg je kippenvel van. Dan denk je echt: wat gebeurt mij hier? Tegelijkertijd is effectieve infiltratie natuurlijk veel beter te organiseren via netwerken dan via apps bij individuele burgers. Daarvoor geldt: goed de privacy in de gaten houden — dat doen we samen met de AP — maar ook dat burgers zich realiseren waar ze op klikken als ze een app downloaden op hun telefoon. Die verantwoordelijkheid zit hier natuurlijk ook achter. Maar dat het 100% veilig is — ik kijk toch elke keer naar meneer Dassen — kun je niet bereiken. Ik ga niet in herhaling vervallen, maar wat wij doen, is op verschillende manieren, op verschillende niveaus, bij wijze van spreken elke dag in de gaten houden wat de risico's zijn en welke maatregelen daarvoor nodig zijn.

Voorzitter. Dan heb ik ook deze vragen inmiddels in mijn algemene betoog en in de interrupties beantwoord. Dan kom ik tot de vraag van volgens mij mevrouw Rajkowski over end-to-end-encryptie om onze veiligheid verder te kunnen vergroten. Het versleutelen van communicatie, encryptie, is natuurlijk een belangrijke methode om vertrouwelijkheid en integriteit van communicatie te borgen. Ik hoef u niet te vertellen dat het kabinet dat ook onderschrijft. In het kader van cybersecurity, kennisontwikkeling en innovatie wordt publiek-privaat een routekaart cryptocommunicatie ontwikkeld. Aan de hand van deze routekaart gaan het bedrijfsleven, de wetenschap en de overheid samenwerken om in het licht van technologische ontwikkelingen, zoals de kwantumcomputer, toekomstbestendige cryptocommunicatiemiddelen ontwikkelen.

Voorzitter. De heer Van der Lee vroeg mij nog naar de diversificatie, die belangrijk is. Hij zei simpel gezegd: voorkom dat je afhankelijk wordt van een of twee bedrijven. Dat zie ik, zeker. Dat is een goed onderwerp om in de gaten te blijven houden. Hoe organiseer je dat met elkaar? Ook hierbij geldt natuurlijk weer — dat is precies in het licht van de woorden die de heer Van der Lee zelf heeft uitgesproken — dat dit ook in het belang is van bedrijven zelf. Je wilt niet afhankelijk zijn van één leverancier, want om te beginnen kan die dan vragen wat die wil. Maar je moet er ook niet aan denken wat er gebeurt als het een keer misgaat.

De **voorzitter**:
Dit roept nog een vraag op bij de heer Van der Lee.

De heer **Van der Lee** (GroenLinks):
Ja, want mijn vraag was nog wel wat specifieker dan dat. De Britse taskforce heeft nadrukkelijk gepleit om open RAN-netwerken te bevorderen. Dat leidt ook tot meer diversiteit. Ze hebben zelfs gezegd: stel een concrete ambitie vast; in 2025 moet ten minste 25% van het netwerk zijn geleverd door kleinere leveranciers of open technologie. De Britten hebben 250 miljoen pond uitgetrokken om dit te stimuleren. Mijn vraag is of dat iets is wat dit kabinet, of het volgende, ook zou willen verkennen. Ik begrijp de uitdaging. Je kunt namelijk niet in China gaan kijken naar al die productiefaciliteiten. Dat klopt. Het is belangrijk om alle risico's in kaart te brengen. Dat klopt ook. Maar het is ook noodzakelijk om in de praktijk aan diversificatie te werken. Anderen hebben daar gericht beleid op. Ik zie dat nog niet in Nederland. Zou de staatssecretaris dat op z'n minst willen verkennen?

Staatssecretaris **Keijzer**:
Dat open RAN is een manier om die diversificatie te bereiken. In EU-verband worden nu de voordelen en de risico's daarvan geanalyseerd. Daar doen wij als Nederland actief aan mee.

Voorzitter. Dan kom ik bij ...

De **voorzitter**:
U kijkt nog even naar de mapjes en dan rent de heer Dassen naar voren voor een interruptie.

De heer **Dassen** (Volt):
Ik heb een hele korte vervolgvraag over dat open RAN. Ik geloof dat daar nog veel verschillende risico's aan kleven. Dat netwerk wordt deels door Chinese staatsbedrijven opgebouwd. Althans, in ieder geval worden de standaarden daarvoor gezet. Ik vraag me af wanneer we dat rapport vanuit de Europese Commissie hier kunnen verwachten.

Staatssecretaris **Keijzer**:
Daar kom ik op terug in tweede termijn.

Voorzitter. De heer Dassen vroeg mij ook om een overzicht van de meest essentiële techbedrijven. Wij brengen voortdurend in kaart wat vitale processen zijn, welke bedrijven daaronder vallen en welke technologie belangrijk is vanuit het oogpunt van toetsing van de investeringen, fusies en overnames. Sensitieve technologie valt onder de reikwijdte van de investeringstoets van de Wet VIFO, de Wet veiligheidstoets investeringen, fusies en overnames. Deze wordt spoedig aangeboden aan de Tweede Kamer.

Voorzitter. Ook werd mij gevraagd hoe we de digitale weerbaarheid van bedrijven vergroten. Ik heb hier een hele tekst voor mij. In ieder geval publiceert het Nationaal Cyber Security Centrum dit jaar gelijktijdig met het Cybersecuritybeeld Nederland — dat was vandaag — de Handreiking Cybersecuritymaatregelen, waarin belangrijke maatregelen worden beschreven die organisaties kunnen treffen. Er is een brochure Cyberspionage. Die biedt organisaties handvatten om hun weerbaarheid te vergroten. Ook op de website van het Digital Trust Center is voor bedrijven informatie te vinden. Daarnaast zijn we nu bezig om het wettelijk mogelijk te maken dat het Digital Trust Center aangewezen kan worden als een OKTT, waardoor bepaalde persoonsgegevens zoals IP-adressen gedeeld kunnen worden. Zo zetten we elke keer weer stappen om bedrijven weerbaar te maken. Daarbij geldt natuurlijk altijd dat ze het

ook wel moeten doen. Daarmee heb ik ook deze vraag beantwoord, volgens mij.

Voorzitter. Ik heb nog twee mapjes. Nou, dat gaat toch vlot. In het eerste mapje zit de vraag van mevrouw Leijten over de visie op de grenzen van publiek en privaat eigendomschap van telecomnetwerken. Daar heb ik al antwoord op gegeven. Ik denk niet dat dat bevredigend is voor mevrouw Leijten, maar het is wel zoals het is.

Aan mij is ook gevraagd om erover na te denken om van standaarden die wij belangrijk vinden als Europese Unie mondiale standaarden te maken. Met de toenemende digitalisering is het natuurlijk van belang ... Nou ja, "toenemende digitalisering", volgens mij zijn de samenleving en de economie allang gedigitaliseerd. Het is van belang om te kijken welke technische standaarden daarvoor nodig zijn. Wij vragen daar als Nederland met gelijkgezinde landen in eerste instantie in EU-verband aandacht en steun voor, maar ook met derde landen wordt internationaal gewerkt aan het steunen van standaardisatievoorstellen die het beste ónze innovatieve ontwikkeling kunnen ondersteunen, bij voorkeur volgens ónze waarden en normen. Wij hebben een wakend oog dat standaarden die we steunen daarbij aansluiten. Het gaat dan bijvoorbeeld om vrijheid, privacy en veilige toegang tot diensten en toepassingen, en zeker niet te vergeten: de menselijke autonomie om te kiezen.

Dank u wel.

De **voorzitter**:
Dank u. Dan kijk ik naar de Kamer. Bent u direct klaar voor de tweede termijn, indien die gewenst wordt? Ik zie geknik. Meneer Dassen, ik zie dat u nog een interruptie heeft. Dan nog een laatste interruptie, staatssecretaris.

De heer **Dassen** (Volt):
Ik had nog een paar andere vragen gesteld. Een van die vragen ging over wat wij van Estland zouden kunnen leren. Estland is namelijk toch in zeer geringe periode koploper op het gebied van cyberveiligheid geworden. Zij hebben een hele digitale overheid en lopen op heel veel gebieden echt voor op de rest van de wereld. Ik ga ervan uit dat we er veel van zouden kunnen leren. Ik ben benieuwd hoe de staatssecretaris daarnaar kijkt en hoe zij daarop actie gaat ondernemen. Dan had ik ook nog een vraag gesteld over de 6G-strategie.

Staatssecretaris **Keijzer**:
De digitale overheid is ook echt weer een ander onderwerp dan het onderwerp dat vandaag in dit debat aan de orde is. Daarnaast is de staatssecretaris van BZK daarvoor verantwoordelijk. Ik denk dat het goed is om het debat met hem te voeren. Dan de 6G. Wij voeren daarover discussies, uiteraard ook weer binnen het Europese, net zoals ik dat voor 5G heb gedaan.

De **voorzitter**:
Ik zie de heer Dassen heftig met zijn hoofd schudden bij de beantwoording van de eerste vraag. Misschien kan hij de vraag verhelderen.

De heer **Dassen** (Volt):
Ja, voorzitter. Het gaat niet over de digitale overheid. Het gaat juist over het onderdeel cyberveiligheid waar Estland flink in vooroploopt. Ik noemde de digitale overheid alleen maar omdat ze daar ook flink in vooroplopen.

Staatssecretaris **Keijzer**:
Wat ikzelf ook persoonlijk trouwens doe, is in de Telecomraad met collega's vanuit de Europese Unie steeds hierover spreken. Daarbij leren we van elkaar. Ik maak ook mee dat staatssecretarissen en ministers uit andere landen aan ons vragen hoe wij het hier doen. Wij vinden het volstrekt normaal dat wij in een structureel overleg zitten met de ministeries, de NCTV, de veiligheidsdiensten en de telecomproviders om door te spreken wat het risicoprofiel is, welke maatregelen elke keer weer nodig kunnen blijken te zijn en ze dan ook te nemen. Dat is iets waar andere landen weer van kunnen leren. Ik begrijp dat de heer Dassen fan is van Estland. Ik weet niet precies wat ze daar dan anders doen dan wij, maar ik ben altijd bereid om te kijken of daar nog iets is dat nog slimmer is dan hoe wij het doen. Dan zal ik echt de eerste zijn om te kijken of het hier ook toegepast kan worden. Maar ik hoop dat ik in mijn uitgebreide betoog over alle maatregelen die wij nemen toch ook de heer Dassen gerustgesteld heb dat we echt het maximale doen. En de heer Dassen is uiteraard zeer welkom bij de technische briefing die ik ook nu weer heb aangeboden.

De heer **Dassen** (Volt):
Ik ben blij om te horen dat de staatssecretaris daarvoor openstaat. Als ik kan, sluit ik natuurlijk aan bij de technische briefing. Ik heb nog een vraag over 6G. Het is goed dat daar al stappen in worden ondernomen. Maar ik ben benieuwd of dat dan ook bij die technische briefing terug gaat komen, of dat we op een andere manier nog worden geïnformeerd over de stappen die daarbij nu worden genomen.

De **voorzitter**:
Tot slot, de staatssecretaris.

Staatssecretaris **Keijzer**:
Daar zijn we mee bezig. Als dat leidt tot voorstellen, zal ik de Kamer daarover informeren. We spreken gewoon af dat we een datum met elkaar zoeken waarop van de achttien fracties die we hebben er vijftien kunnen. Dan moet dat lukken. Als de heer Dassen dan nog niet kan, dan krijgt hij een persoonlijke briefing van de betrokken personen.

De **voorzitter**:
Een personal treatment. Heel goed.

Staatssecretaris **Keijzer**:
Dank u.

De **voorzitter**:
Dank. Dan geef ik allereerst voor de tweede termijn mevrouw Van Ginneken van D66 het woord.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter. Het was een uitgebreide uitwisseling, maar ik moet ook constateren dat de vragen die ik heb gesteld over zekerheid bij de opschoning van ons mobiele telecomnetwerk onvoldoende beantwoord zijn. Ik denk dat onze samenleving meer duidelijkheid mag verwachten. Daarom heb ik twee moties.

De eerste motie.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de inlichtingen- en veiligheidsdiensten al jarenlang waarschuwen voor het risico op spionage via het mobieletelefonienetwerk;

overwegende dat bedrijven, wetenschappers, journalisten, mensenrechtenactivisten en alle andere mensen in onze samenleving veilig en vertrouwelijk moeten kunnen communiceren;

overwegende dat de samenleving het recht heeft te weten wanneer het mobieletelefonienetwerk weer veilig en vertrouwelijk is;

verzoekt de regering de termijn waarop mobieletelecomaanbieders hun netwerk opgeschoond moeten hebben openbaar te maken en aan te geven of hier aan mobieletelecomaanbieders compensatie voor geboden is,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Van Ginneken, Van der Lee en Kathmann.

Zij krijgt nr. 144 (30821).

Mevrouw **Van Ginneken** (D66):
De tweede motie.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de inlichtingen- en veiligheidsdiensten al jarenlang waarschuwen voor het risico op spionage via het mobieletelefonienetwerk;

overwegende dat het voor de Kamer noodzakelijk is om te weten of het recht op veilige en vertrouwelijke communicatie op tijd hersteld is;

verzoekt de regering direct na de datum waarop mobieletelecomaanbieders hun netwerk opgeschoond moeten hebben een audit uit te voeren of de netwerken adequaat opgeschoond zijn, en de Kamer daarover te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Van Ginneken, Van der Lee, Kathmann en Rajkowski.

Zij krijgt nr. 145 (30821).

Dank u.

Mevrouw **Van Ginneken** (D66):
Dank u wel.

De **voorzitter**:
Dan geef ik het woord aan mevrouw Leijten van de SP.

Mevrouw **Leijten** (SP):
Voorzitter. Het is geen heel technisch debat geworden, wat dan soms de principiële vraag omzeilt: als je het over de techniek hebt, heb je het niet meer over het waarom. Tegelijkertijd is het wel weer een vaag debat geworden. We hebben heel veel vragen gesteld: wat zijn nou de strategische keuzes die we met z'n allen maken en hoe kunnen we daar controle op uitoefenen en toezicht op organiseren? Maar dat wordt afgedaan als vertrouwelijk. Dan hebben we wel een probleem, maar dit probleem is groter en breder dan alleen deze staatssecretaris en dit onderwerp. Aankomende maandag spreken we er ook over met de coördinerend bewindspersoon, zoals dat dan heet, de hoofdverantwoordelijke. De SP heeft al een voorstel gedaan dat voortaan door zowel Kamerleden als experts en de rijksoverheid wordt bekeken wat staatsgeheim is, wat niet gedeeld kan worden en hoe daarin afwegingen worden gemaakt. Het is mijn grote overtuiging dat de regering dat niet alleen kan besluiten. Zo zit simpelweg onze Grondwet niet in elkaar.

Verder verwijst de minister, of de staatssecretaris — wie weet voor de toekomst? — mij door naar een volgend kabinet, als het gaat over visie. Nou weet ik welke twee partijen nu met elkaar gezellig zitten te schrijven. Ik heb daarbij niet zo heel veel hoop op een visie, maar wie weet horen de woordvoerders het en kunnen ze het meegeven. Want ik denk wel dat het tijd is dat we het gaan doen. Als de regering het niet gaat doen, dan gaat de nieuwe commissie voor Digitale Zaken het zeker wel doen.

De **voorzitter**:
Dank u. Dan kijk ik naar mevrouw Kathmann van de PvdA.

Mevrouw **Kathmann** (PvdA):
Voorzitter. Ik deel de mening van mevrouw Leijten dat het een moeilijk debat is. We zitten hier met de staatssecretaris van Economische Zaken, die volgens mij al het mogelijke heeft gedaan wat in haar macht ligt. Daarom ligt er ook zo'n mooie Europese toolbox.

Aan de andere kant spreken we hier gewoon over onze nationale veiligheid. Dat is geen economisch vraagstuk dat alleen maar gaat over open markten, maar het vraagt om een sterke overheid die ingrijpt om burgers te beschermen. De staatssecretaris zei het zelf ook al: daar zit een ongelofelijke spanning op. De Partij van de Arbeid erkent die spanning, maar we willen toch dat Nederland een stapje verder zet, al erken ik ook de opmerking van de heer Dassen. Iedereen die zegt "joh, we bannen even wat tech uit derde landen en dan is het veilig" heeft boter op zijn hoofd. 100% veilig bestaat niet en heel veel technologische maakindustrie van Europese bedrijven vindt juist plaats in die landen die we proberen te bannen.

De Partij van de Arbeid vindt wel, al bestaat 100% veilig niet, dat je altijd moet willen blijven streven naar de optimale variant van veiligheid. Inmenging in onze digitale infrastructuur door landen die wij niet vertrouwen hoort daar gewoonweg niet bij. Maar ik deel dan ook weer de mening van de staatssecretaris dat het moeilijk is om zo'n lijst vast te stellen. Die moet dynamisch zijn. Je kan niet zeggen "dan gaan we dat maar even weren", want vervolgens is er weer een nieuw bedrijf opgericht en dat gaat dan niet. Het is dus een dynamische lijst, maar we zouden het wel moeten willen. Eigenlijk zijn het dezelfde stappen die een land als België zet. Dat zegt: die toolbox is er, maar we doen een tandje harder. Die bedrijven zijn gewoon niet welkom, bijvoorbeeld in de haven van Antwerpen. Maar neem ook een land als Spanje, dat wel de tech uit derde landen die we niet vertrouwen in de ban doet. Daar horen twee moties bij, de ene iets verdergaand dan de andere. Ik zal ze zo snel mogelijk voorlezen.

De **voorzitter**:
Ja, dit loopt weer totaal uit de klauwen. Uptempo!

Mevrouw **Kathmann** (PvdA):
Heel kort.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat bedrijven uit landen die we niet vertrouwen technologie leveren voor de Nederlandse digitale infrastructuur;

constaterende dat Europese bondgenoten bedrijven weren om de (digitale) veiligheid te waarborgen;

overwegende dat Europese bondgenoten die bedrijven niet volledig weren dit bijvoorbeeld wel doen als het gaat om cruciale infrastructuur;

draagt de regering op om ervoor te zorgen dat bedrijven van landen die we niet vertrouwen geen toegang meer krijgen tot de digitale infrastructuur;

draagt de regering op om te zorgen voor uitfasering van bedrijven uit die landen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 146 (30821).

Mevrouw **Kathmann** (PvdA):
Dan een iets minder verregaande, die van tevoren helemaal hetzelfde zegt.

Motie

De Kamer,

gehoord de beraadslaging,

verzoekt de regering in kaart te brengen wat er nodig is om deze bedrijven te weren van de digitale infrastructuur,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 147 (30821).

Dank u. Een tip voor de volgende keer: begin gewoon met de moties en dan kunnen de vragen daarna. Dan geef ik het woord aan mevrouw Rajkowski van de VVD. Geen behoefte. Dan mevrouw Van Dijk van het CDA.

Mevrouw **Inge van Dijk** (CDA):
Dank u wel, voorzitter. Het is door een aantal mensen al genoemd. Het was een best wel lastig debat omdat het enerzijds gaat over de portefeuille van de staatssecretaris maar het onderwerp anderzijds ook honderdduizend andere vraagstukken oproept, bijvoorbeeld over veiligheid, over hoe je de concurrentie voorblijft en over hoe je dienstverlening voor onze burgers waarborgt. Het is ingewikkeld.

Een onderwerp dat door meerdere leden is aangekaart, is vertrouwelijkheid. Wat brengen we wel en wat brengen we niet naar buiten? Ik dacht dat ik een toezegging had gehoord van de staatssecretaris. Ja, natuurlijk wil ik graag nog eens een keer praten over wat vertrouwelijk is en wat niet. Ik denk dat we die discussie breder moeten trekken. We moeten die niet voeren en dan weer stoppen. Volgens mij moet je haar regelmatig herhalen, omdat je ziet dat we in de loop der tijd er steeds anders mee omgaan.

Ik had een vraag gesteld over de apps en de mobiele toestellen. De staatssecretaris gaf het al aan: ze kreeg er kippenvel van. Misschien raakt het niet direct aan dit debat, maar ik heb er toch een motie over voorbereid, omdat het wel gewoon een actueel onderwerp is.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat telecommunicatie kwetsbaar is voor spionage, afluisteren, infiltratie en sabotage;

overwegende dat thans de focus ligt op maatregelen ter bescherming van de veiligheid en integriteit van mobiele telecommunicatienetwerken, terwijl de rol van cyberveiligheid bij (het gebruik van) apps en mobiele toestellen veel minder aandacht krijgt;

overwegende dat door verkeerd gebruik of via "achterdeurtjes" in populaire, veel gebruikte apps als het Chinese TikTok kwaadwillenden kunnen binnendringen in de levens van mensen, onder wie kinderen, om persoonlijke informatie te verzamelen, te verhandelen of tegen henzelf of anderen te gebruiken;

overwegende dat de Consumentenbond en de stichting Take Back Your Privacy een claim tegen TikTok hebben ingediend wegens het jarenlang illegaal verzamelen en verhandelen van gebruikersgegevens;

verzoekt de regering ter aanvulling op de genomen en geplande stappen uit de Kamerbrief van 16 juni 2021 (2021D23601) een analyse te maken van de rol van cyberveiligheid bij (het gebruik van) apps en mobiele toestellen, en risico's en kwetsbaarheden in kaart te brengen;

verzoekt de regering daarbij expliciet aandacht te besteden aan hoe kinderen beter zouden kunnen worden beschermd,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Inge van Dijk.

Zij krijgt nr. 148 (30821).

Dank u. Dan geef ik het woord aan de heer Van der Lee van GroenLinks.

☐

De heer **Van der Lee** (GroenLinks):
Dank, voorzitter. En ook dank aan de staatssecretaris voor de beantwoording. Ik deel dat het een wat ingewikkeld debat is. Het onderzoek van de toezichthouder naar de aanleiding is nog niet beschikbaar, het kabinet is demissionair en we hebben eigenlijk best wel allemaal wensen. Terechte wensen, want ik ben niet gerustgesteld en, eerlijk gezegd, zou ook niemand dat moeten zijn. We moeten blijvend waakzaam zijn op dit terrein. Ook dat zijn we het volgens mij met elkaar eens.

Ik wil nog wel graag een antwoord op mijn vraag — die zou de staatssecretaris in tweede termijn beantwoorden — of het nu onderdeel is van de zorgplicht dat de providers, als zij dingen tegenkomen, dat ook proactief moeten melden aan de toezichthouder. We moeten een vinger aan de pols houden. Dat kunnen we niet als Kamer direct. Daar hebben we anderen voor. Maar we moeten wel de garantie hebben dat die interactie plaatsvindt.

Op één punt dien ik een motie in.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de diversiteit van leveranciers van telecominfrastructuur de weerbaarheid van het telecomnetwerk ten goede kan komen;

overwegende dat de ontwikkeling en het gebruik van Open RAN-technologie snel toeneemt, bijvoorbeeld in het Verenigd Koninkrijk, de Verenigde Staten en Japan;

overwegende dat het van belang is dat ook Europese bedrijven bij deze ontwikkeling aangehaakt blijven;

verzoekt de regering te onderzoeken op welke wijze het gebruik van Open RAN-technologie in het Nederlandse telecomnetwerk bevorderd zou kunnen worden en wat de voordelen en nadelen hiervan zijn,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Van der Lee en Van Ginneken.

Zij krijgt nr. 149 (30821).

De heer **Van der Lee** (GroenLinks):
En ik hoop ook dat dat Europese onderzoek dan ook snel gepaard gaat met beleidsaanbevelingen — waarschijnlijk door het nieuwe missionaire kabinet — en dat op die manier wel uitvoering aan deze motie kan worden gegeven.

Daarbij houd ik het. Dank u wel, voorzitter.

De **voorzitter**:
Dank u. De heer Dassen heeft geen behoefte aan een tweede termijn. Ik kijk even naar de staatssecretaris. Tien minuutjes schorsen? Dan komen we rond de klok van negen weer bij u terug.

De vergadering wordt van 20.52 uur tot 21.04 uur geschorst.

De **voorzitter**:
Het woord is aan de staatssecretaris voor de overgebleven vragen en de beoordeling van de moties.

☐

Staatssecretaris **Keijzer**:
Voorzitter. De vraag die mij in de eerste termijn nog werd gesteld door de heer Van der Lee was of er een meldplicht is voor incidenten. Die is er. Aanbieders van openbare elektronische communicatienetwerken en -diensten moeten een inbreuk op de veiligheid of integriteit melden bij Agentschap Telecom wanneer de continuïteit van deze openbare netwerken en diensten in belangrijke mate wordt onderbroken. Vanaf een bepaalde omvang en uiteraard bij situaties waar uitval van 112 aan de orde is, moeten deze

dus worden gemeld. Dus dat is richting de heer Van der Lee.

De heer Dassen van Volt vroeg aan mij wanneer ik het Europese rapport over de analyse van kansen en risico's van open RAN kan verwachten. Dat is eind dit jaar.

Mevrouw Van Ginneken vroeg aan mij wanneer de brieven waarin de beschikkingen zaten verstuurd werden. Ik had daar de datum niet van paraat. Maar dat was kort na het vragenuurtje, namelijk op 23 april van dit jaar. Dat waren volgens mij de vragen.

Dan kom ik nu bij de moties. De eerste is de motie-Van Ginneken c.s. die verzoekt om de termijn waarop mobiele telecomaanbieders hun netwerk moeten hebben opgeschoond openbaar te maken en aan te geven of hier aan telecomaanbieders compensatie voor geboden is. Ik moet deze motie ontraden. Het eerste betreft bedrijfsvertrouwelijke en staatsgeheime informatie. Ik kan dat dus gewoon niet met u delen. Ten aanzien van nadeelcompensatie kan ik dat pas beantwoorden nadat de aanvraag daarvoor is gedaan door de providers en daarover is besloten.

Mevrouw **Van Ginneken** (D66):
Ik begrijp nog steeds niet zo goed waarom de staatssecretaris die termijn niet bekend kan maken. Ik hoor ook nog steeds geen toelichting waarom die datum zo'n probleem is, dus het blijft een beetje een schimmenspel. Ik zou heel graag met de samenleving, met journalisten en met experts het gesprek kunnen voeren over de vraag of wij kunnen leven met een zekere termijn waarop ons mobiele telecomnetwerk weer als veilig beschouwd mag worden. Ik denk dat die transparantie juist in het belang van de nationale veiligheid gegeven kan worden. Dus ik heb het idee dat de staatssecretaris die hier juist niet dient. Ik verzoek de staatssecretaris dus de appreciatie te heroverwegen.

Staatssecretaris **Keijzer**:
Wat deel ik niet?

Mevrouw **Van Ginneken** (D66):
Excuus, dan ben ik niet helemaal duidelijk. Ik had het over de termijn waarop mobiele telecomaanbieders hun netwerk opgeschoond moeten hebben.

Staatssecretaris **Keijzer**:
Klopt. Ik dacht dat ik nu beluisterde dat ik niet deelde dat het belangrijk is dat de maatschappij vertrouwen kan hebben in deze netwerken. Ik dacht: wat hebben we hier dan de afgelopen twee uur gedaan? Maar dat was gelukkig niet wat mevrouw Van Ginneken zei.

Mevrouw **Van Ginneken** (D66):
Dat is niet wat ik wilde zeggen. En ik zal nog even terugkijken of ik dat mogelijk toch heb gezegd.

Staatssecretaris **Keijzer**:
Het ligt vast bij mij. Daarom vraag ik het ook maar meteen. Dan is dat in ieder geval meteen uit mijn systeem, dus dat is fijn. Want ik vind dat natuurlijk ook. We hebben beschikkingen gestuurd. Daarin zitten maatregelen die de providers moeten nemen. Privacy is een groot goed, ook voor de fractie van D66. Dat gaat vaak over persoonsgegevens, maar natuurlijk ook over bedrijfsvertrouwelijke informatie. Die mag ik niet delen. Dat is ook een van de gronden op basis waarvan je geen openbaarheid kunt betrachten in het kader van openbaarheid van bestuur. Daarnaast heb je nog staatsgeheimen. Ik kan dat gewoon niet doen. Ik hoop dat mevrouw Van Ginneken, die ook bij die technische briefing is geweest en daar gehoord heeft hoe het allemaal precies in elkaar steekt, dat gewoon wil zien. Anders moet ze een discussie voeren met de bewindspersonen die gaan over de AIVD en de MIVD. Dat zijn de minister van BZK, mevrouw Ollongren, en de minister van Defensie, mevrouw Bijleveld. Ik kan het gewoon niet mooier maken, maar laten we hier ook niet net met elkaar doen alsof dit kabinet niet de juiste maatregelen heeft genomen, want dat hoor ik mevrouw Van Ginneken ook niet zeggen. Daar ben ik dan in ieder geval blij mee.

De **voorzitter**:
U ziet het, mevrouw Van Ginneken. De appreciatie is niet veranderd. Daar blijft het oordeel bij.

Staatssecretaris **Keijzer**:
In de motie-Van Ginneken c.s. op stuk nr. 145 vraagt zij om na de datum waarop mobieletelecomaanbieders hun netwerk opgeschoond moeten hebben, een audit uit te voeren of dat adequaat gebeurd is. Deze laat ik oordeel Kamer. Agentschap Telecom houdt toezicht op de uitvoering van de beschikking en zal controleren of hier invulling aan wordt gegeven.

In haar motie op stuk nr. 146 draagt mevrouw Kathmann de regering op om bedrijven uit landen die we niet vertrouwen, uit te faseren uit de digitale infrastructuur. Ik ontraad deze motie. Ik heb uitgebreid uiteengezet hoe wij komen tot onze maatregelen. Dat is op basis van risicoanalyses.

In haar motie op stuk nr. 147 verzoekt mevrouw Kathmann de regering in kaart te brengen wat er nodig is om bedrijven te weren van de digitale infrastructuur. Ook deze ontraad ik, ook in het licht van de manier waarop wij onze aanpak vormgegeven hebben. Daarbij hoort het niet om a priori bedrijven te gaan weren.

Dan kom ik op de motie van mevrouw Van Dijk van het CDA over de TikTok-app. Dat is de motie op stuk nr. 148. We hebben het net in de eerste termijn ook gedeeld: als je dat verhaal van mevrouw Van Dijk hoort, krijg je toch een beetje kippenvel. De Autoriteit Persoonsgegevens doet uiteraard ook onderzoek naar privacy. Alleen, de problematiek van spionage en mogelijke sabotage van mobiele telecomnetwerken en statelijke actoren is niet hetzelfde als de veiligheid en de privacy van kinderen bij het gebruik van apps zoals TikTok. Ze zijn beide relevant, maar niet direct aan elkaar gelinkt. Informatie van inlichtingendiensten over spionage en sabotage van statelijke actoren vormt een belangrijke sturing om onze capaciteit te focussen en geconstateerde dreigingen het hoofd te bieden. Voor veiligheid en privacy, in het bijzonder van kinderen, geldt dat wij nadrukkelijk inzetten op een breed scala en maatregelen, waaronder passende wettelijke waarborgen voor cybersecurity en privacy, initiatieven op het gebied van publiek-

private samenwerking en voorlichting en toezicht. Ik heb dat in de eerste termijn ook aangegeven. Zoals gezegd doet de AP onderzoek naar apps en privacy. De Europese algemene verordening gegevensbescherming is dan ook van toepassing. Op dit moment zijn we binnen het Europese verder aan het onderhandelen in het kader van de e-privacyverordening. Collega-minister Dekker voor Rechtsbescherming heeft op verzoek van het lid Ceder toegezegd de Kamer dit najaar te informeren over de mogelijkheid om de bescherming van persoonsgegevens van kinderen te intensiveren. Kortom, er gebeurt veel. Het kabinet blijft hierop inzetten. Dat maakt voor mij dat ik tegen mevrouw Van Dijk kan zeggen dat deze motie het beleid zeer ondersteunt en dat ik het oordeel over de motie aan de Kamer kan laten.

Dan kom ik bij de motie op stuk nr. 149 van de heer Van der Lee. Hij vraagt mij daarin om te onderzoeken op welke wijze het gebruik van Open-RAN-technologie in het Nederlandse telecomnetwerk bevorderd zou kunnen worden en wat de voor- en nadelen hiervan zijn. Het is een interessante ontwikkeling die ziet op de diversificatie die van belang is. Er wordt gewerkt aan een analyse van de risico's en de voordelen van deze Open RAN. Het resultaat zal mogelijk bijdragen aan de gezamenlijke aanpak van de Unie voor de beveiliging van 5G-netwerken, onder andere door middel van de verdere ontwikkeling van de zogeheten toolbox for 5G security. Daar doen we actief aan mee. Ik zie deze motie dan ook als ondersteuning van beleid, waarvoor dank, en ik laat het oordeel erover aan de Kamer.

De **voorzitter**:
Dank.

De beraadslaging wordt gesloten.

De **voorzitter**:
De stemmingen zijn volgende week dinsdag. Ik dank de staatssecretaris, de leden en de bodes. Ik wens u een goede avond.