Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

30 821 Nationale Veiligheid

Nr. 90

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 17 juli 2019

De vaste commissie voor Justitie en Veiligheid en de vaste commissie voor Buitenlandse Zaken hebben op 20 juni 2019 overleg gevoerd met de heer Grapperhaus, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 9 januari 2019 inzake onderzoek «Op weg naar een Weerbare Open Samenleving» (Kamerstuk 30 821, nr. 52);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 25 maart 2019 inzake uitfasering van het Waarschuwings- en Alarmeringssysteem (Kamerstuk 29 517, nr. 167);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 15 april 2019 inzake reactie op het verzoek van lid Klaver, gedaan tijdens de regeling van werkzaamheden van 3 april 2019, over de vernieuwing en beveiliging van het C2000 spraaknetwerk en de uitrol van 5G, voordat onomkeerbare besluiten worden genomen (Kamerstukken 25 124 en 24 095, nr. 94);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 16 april 2019 inzake rapport «Evaluatie van (het gebruik van) de Risicokaart» (Kamerstuk 30 821, nr. 71);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 18 april 2019 inzake tegengaan statelijke dreigingen (Kamerstuk 30 821, nr. 72);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 26 april 2019 inzake auditrapport van Xebia met betrekking tot de beveiliging van het vernieuwde C2000 (Kamerstuk 25 124, nr. 95);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 26 april 2019 inzake beveiliging nieuwe infrastructuur mobiele communicatie (C2000) (Kamerstuk 25 124, nr. 96);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 7 juni 2019 inzake Nationale Veiligheid Strategie 2019 (Kamerstuk 30 821, nr. 81);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 12 juni 2019 inzake Cybersecuritybeeld Nederland 2018 (CSBN 2018) en voortgangsrapportage NCSA (Kamerstuk 26 643, nr. 614);**

kst-30821-90
ISSN 0921 - 7371
's-Gravenhage 2019

– **de brief van de Minister van Justitie en Veiligheid d.d. 12 juni 2019 inzake voortgang integrale aanpak cybercrime (Kamerstuk 28 684, nr. 564).**

Van dit overleg brengen de commissies bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
Van Meenen

De voorzitter van de vaste commissie voor Buitenlandse Zaken,
Pia Dijkstra

De waarnemend griffier van de vaste commissie voor Justitie en Veiligheid,
Tiekens-Tripels

Voorzitter: Van Meenen
Griffier: Freriks

Aanwezig zijn vijf leden der Kamer, te weten: Buitenweg, Van Dam, Laan-Geselschap, Van Meenen en Verhoeven,

en de heer Grapperhaus, Minister van Justitie en Veiligheid.

Aanvang 12.34 uur.

De **voorzitter**:
Goedemiddag. Ik open het algemeen overleg van de vaste Kamercommissie voor Justitie en Veiligheid. Het onderwerp van vandaag is nationale veiligheid en crisisbeheersing. Ik heet de Minister en zijn ambtenaren van harte welkom, zo ook de leden, de mensen op de publieke tribune en onze ondersteuning. We hebben afgesproken uiterlijk tot 15.30 uur hierover met elkaar te spreken. We hebben daarom spreektijden van vier minuten. Het aantal leden is nog beperkt, maar dat zal ongetwijfeld toenemen. Laten we beginnen met twee interrupties per persoon. Als u daarmee kunt instemmen, geef ik als eerste het woord aan mevrouw Buitenweg van GroenLinks.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, meneer de voorzitter. Bij dit AO Nationale veiligheid staan ontzettend veel verschillende onderwerpen op de agenda. Ik kan daar niet allemaal recht aan doen en heb er een aantal uit gepakt die mij het meest na aan het hart liggen. Het eerste daarvan is C2000. Het huidige communicatiesysteem voor hulpverleners is toe aan vervanging, heel erg urgent zelfs, lezen we. Het is nu houtje-touwtje en dat maakt het systeem minder betrouwbaar en minder veilig. Ook over het voorgestelde nieuwe systeem bestaat maar beperkt enthousiasme, volgens de AIVD-brieven. De AIVD zegt: ja, we kunnen wel overgaan naar dit nieuwe systeem, maar laten we parallel aan de migratie starten met een vervangingstraject. Het systeem werkt nog niet, maar we worden nu al gevraagd om te kijken naar vervanging van dat systeem. Dat is waar we staan. Ik vraag de Minister hoe lang de bedoeling was dat C2000 zou meegaan. Wat was het oorspronkelijke plan? Wat verandert dit advies van de AIVD aan die levensverwachting van C2000? Ik lees in de brief dat de Minister het advies van de AIVD overneemt. Betekent dit dat nu al de eerste stappen zijn gezet om het nieuwe C2000 op zo kort mogelijke termijn te vervangen? Neemt de Minister ook het advies over om een nieuw systeem minder afhankelijk te maken van bedrijven die gelinkt zijn aan China?
In het afgelopen jaar is veel gezegd over Huawei en Hytera. Ik wil het vandaag hebben over een ander Chinees bedrijf: Hikvision, de grootste beveiligingsproducent ter wereld met het Europese hoofdkantoor in Hoofddorp. Het is een voorloper op het gebied van gezichtsherkenning en kunstmatige intelligentie. Dagelijks rollen er 260.000 camera's van de lopende band en het laat zich erop voorstaan de bewegingen van een persoon door het hele land te kunnen volgen en mensen te kunnen herkennen aan de manier waarop ze lopen. Hikvision is voor 42% in handen van de Chinese staat en nauw betrokken bij het allesomvattende surveillancesysteem in de regio Xinyang. Via slimme camera's, die bijvoorbeeld raciale kenmerken kunnen herkennen, helpen ze om de Oeigoeren daar te onderdrukken. Dankzij de banden met de Chinese communistische partij heeft dit bedrijf snel kunnen groeien. Het heeft goedkoper kunnen lenen en de producten tegen een lage prijs op de markt kunnen brengen, ook in het Westen. We weten inmiddels dat Britse straten, bussen en ziekenhuizen er vol mee hangen. Hoe is dat in Nederland? Is de Minister het met mij eens dat het ongewenst is dat de

overheid Hikvision verder in het zadel helpt? Dezelfde vraag geldt voor het bedrijf Dahua, dat ook via gezichtsherkenning helpt om Oeigoeren in interneringskampen te houden. De Verenigde Staten willen deze bedrijven op een zwarte lijst zetten zodat zij geen Amerikaanse technologie kunnen kopen. Hoe staat Nederland hierin? Zijn daar richtlijnen voor? Is de Minister bereid om de Tweede Kamer te informeren over het gebruik in Nederland van producten van Chinese bedrijven die op de Amerikaanse sanctielijst staan, met name door de Nederlandse publieke en semipublieke instellingen?

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

Mevrouw **Laan-Geselschap** (VVD):
Voorzitter, dank. Als dit systeem niet door een Chinees bedrijf zou worden geproduceerd maar door een Nederlandse bedrijf, zou GroenLinks er dan voor in zijn om dit soort instrumenten in te zetten bij de opsporing van terroristen?

Mevrouw **Buitenweg** (GroenLinks):
Ik denk dat dit een van de onderwerpen is die we goed met elkaar moeten gaan bespreken. Er zijn plekken, zoals in San Francisco, waar ze hebben gezegd: we moeten helemaal niet overgaan naar gezichtsherkenning omdat dit te grote problemen geeft voor de publieke vrijheden. Ik denk dat dat een onderwerp is – het principe van gezichtsherkenning, het gebruik van camera's en het op die manier de hele tijd iedereen in kaart brengen – waarvan we met elkaar de vraag moeten stellen of dat past bij de vrije samenleving waar we voor staan. Ik heb daar grote twijfels bij.

Mevrouw **Laan-Geselschap** (VVD):
Ik zou dat graag onderzocht willen hebben. Het is een deel van mijn spreektekst, dus ik kom daar later nog even op terug. Dank voor uw reactie.

De **voorzitter**:
Dank u. Een interruptie van de heer Verhoeven van D66.

De heer **Verhoeven** (D66):
Goed punt wel van GroenLinks. Ik ben het eens met de benadering die ik in de woorden van mevrouw Buitenweg hoor. Maar wat is nu precies het punt dat GroenLinks wil maken met betrekking tot dit AO? Ik zoek even naar de verhouding tussen aan de ene kant de principiële discussie over het cluster gezichtsherkenning, camera's, surveillance en privacyveiligheid, en aan de andere kant de zorgen die GroenLinks al eerder heeft geuit over afhankelijkheid, China, technologie, positie van Nederland en vitale infrastructuur, en de overlap daartussen.

Mevrouw **Buitenweg** (GroenLinks):
Meneer Verhoeven heeft gelijk dat het eigenlijk om meerdere punten draait. Het gaat inderdaad om de principiële discussie die we urgent met elkaar moeten voeren over gezichtsherkenning en op welke wijze we onze vrijheden gaan garanderen. Het gaat inderdaad ook om de vraag in welke handen iets is. Dat raakt aan het punt of het anders zou zijn als het in Europese handen is. Voor mij is dat wel zo. In Europa weet je zeker dat daarop meer checks-and-balances van toepassing zijn zoals wij die in Europa hebben vastgesteld. Dat brengt me bij de vraag van wat we nou moeten doen. De NCTV heeft ook gezegd dat Europese landen te afhankelijk zijn van maar een paar aanbieders. Dat geldt voor de soft- en hardware van allerlei producten, ook van C2000 en 5G. Hoe gaan we daarmee om? We kunnen niet aan de gang blijven om alleen maar zaken

te verbieden of daarover onze zorgen te uiten. Ik denk dat het nodig is dat we in Europa meer aan een eigen Europese industrie gaan bouwen. Dat is ook een vraag die ik aan de Minister wil stellen. Op welke wijze ga je stimuleren dat we eigen Europese aanbieders hebben? Speelt zoiets ook een rol bij een aanbesteding? Te vaak kijken we naar de korte termijn. Wat is het goedkoopste product? Welk product is state-of-the-arttechnologie? Dan kan je al gauw sneller uitkomen bij een bedrijf in China. Tegelijkertijd bestendig je dan een trend dat China de koploper is, terwijl je eigenlijk wilt dat we daarin ook in Europa veel meer gaan investeren. Dat is dus ook een vraag die ik aan de Minister wil stellen. Op welke wijze speelt zoiets, die wens, nou een rol bij een aanbestedingstraject?

De **voorzitter**:
De heer Verhoeven nog, wellicht. Nee? Helder?

De heer **Verhoeven** (D66):
Nee, nee, ik was even op zoek naar deze woorden.

De **voorzitter**:
Goed. Mevrouw Buitenweg, gaat u verder. U heeft nog een minuut.

Mevrouw **Buitenweg** (GroenLinks):
Dan ga ik heel snel over naar een aantal andere vragen die ik heb. Hebben wij de technische kennis en inlichtingenkennis om te weten uit welk land een cyberaanval komt? Aan de ene kant willen we dat weten om te zorgen dat een land schade krijgt door het in verlegenheid te brengen, de attribution, maar we willen natuurlijk ook voorkomen dat iemand het gebruikt zodat wij eigenlijk het verkeerde land aanwijzen. Dus hebben wij die knowhow, zowel technisch als qua inlichtingen, om dat te doen en te voorkomen dat wij een verkeerd land aanwijzen? Want juist in deze tijd van toenemende bewapening lijkt me dat ook een risico.
Dan wil ik het hebben over het Cybersecuritybeeld. Daarin zien we dat we extra kwetsbaar zijn, omdat we geen analoge alternatieven hebben. We hebben geen terugvalopties. Met name één voorbeeld bleef me bij: onze bankrekeningen. Zijn er back-ups van de saldi van onze bankrekeningen? Of zouden die in het geval van een aanval ook gemanipuleerd zijn? Toen las ik dat het antwoord hierop lastig te geven is. Daar werd ik toch een beetje zenuwachtig van. Ik vraag me af of de Minister daar ook naar kan kijken.
Dan rond ik af, voorzitter, met de weerbaarheid van de rijksoverheid zelf. Die is verslechterd ten opzichte van 2017, las ik. Rijkswaterstaat heeft bijvoorbeeld de afgelopen jaren veel beter in kaart gebracht wat nodig is om waterkeringen beter te beveiligen, maar heeft dit niet gedaan. Vindt deze coördinerend Minister dat zijn collega's het onderwerp voldoende prioriteit geven en wat is zijn rol daarin?

De **voorzitter**:
Dank u zeer. Dan is het woord aan mevrouw Laan van de VVD.

Mevrouw **Laan-Geselschap** (VVD):
Dank, voorzitter. Om maar gelijk aan te sluiten bij de collega: bij het fenomeen cybersecurity is continu een permanente afweging te maken tussen een open samenleving aan de ene kant en de roep om bevoegdheden van de overheid om maatregelen te nemen om die veiligheid te garanderen aan de andere kant. De VVD kiest voor veiligheid, maar nadrukkelijk met het in beeld houden van privacy. Veiligheid, want als het goed mis gaat met cybersecurity, dan gaat het ook echt heel goed mis.
Ik zie hier ook kansen voor de bv Nederland. We zijn een land dat veel kennis in huis heeft in combinatie met een gezonde handelsgeest. Er liggen kansen voor ondernemers en wetenschappers. Daarom zouden

centraal geregelde budgetten voor de ontwikkeling van instrumenten en kennis om dit soort criminaliteit tegen te gaan, voor ons heel welkom zijn. Die hebben we nog niet. Mijn vraag aan de Minister, via u, voorzitter, is of het niet tijd is om dit in Nederland goed te gaan regelen. Als overheid kunnen we als katalysator dergelijke ontwikkelingen op gang brengen. Een percentage van de 95 miljoen die nu jaarlijks beschikbaar is voor cybercrime en ondermijning zou hiervoor uitermate geschikt zijn. En niet alleen voor meer mankracht zoals nu aan de orde is. Want voor dit soort criminaliteit is meer mankracht alleen niet een oplossing, structureel werken aan de verbetering van de kennispositie daarentegen wel. Hoe kijkt de Minister hiertegen aan?
Voor veel Nederlanders is mijn tweede onderwerp waarschijnlijk veel tastbaarder dan het vorige. Dit gaat over het waarschuwings- en alarmsysteem, oftewel de bekende sirene op de eerste maandag van de maand, toch een beetje een nationaal moment van eenheid. Er is besloten dat op termijn NL-Alert, dat via de mobiele telefoon verspreid wordt, dit alarmsysteem gaat vervangen. In de Kamer is destijds afgesproken dat de sirenes pas uitgaan als het nieuwe systeem in heel Nederland voldoende bereik heeft. Dat is nu nog steeds niet het geval, want er is een dekking van 75%. Het heeft mijn voorkeur om beide systemen naast elkaar te laten bestaan. Kan dit, Minister? Wat is daarvoor nodig? Wanneer er nu binnenkort serieus iets misgaat, bij bijvoorbeeld een fabriek, hebben we die sirenes echt nog steeds keihard nodig. Samen met collega Buitenweg heb ik veelvuldig gehamerd op het belang van een veilig communicatiesysteem voor onze hulpdiensten, C2000, u heeft er net al over gehoord. Buitenlandse spionage en inmenging in dit systeem is ontoelaatbaar. Ik ben dan ook tevreden met het uitgevoerde veiligheidsonderzoek. Opvallend is echter dat de AIVD adviseert om ondanks alle genomen maatregelen op termijn toch over te stappen op een nieuwe leverancier. Ik wil graag van de Minister weten welke kosten hiermee gemoeid zijn en waarom de overstap op een volledig betrouwbare leverancier dan nu niet kan gebeuren. De Minister lijkt de problemen een beetje door te schuiven naar zijn opvolger.
Aansluitend bij het begin van mijn verhaal, de cybersecurity: Nederland gaat zich in de EU inzetten voor gezamenlijke actie op het gebied van cyberveiligheid en het communicatiesysteem om sowieso minder afhankelijk te worden van Chinese en Amerikaanse technologie en leveranciers. Zo ja, gaat dit gebeuren en waar zet Nederland dan op in? Is de Minister bereid om de financiële gevolgen te dragen wanneer blijkt dat de veilige keuzes duurder zijn dan de goedkoopste keuzes, oplossingen en leveranciers? Hier is net al aan gerefereerd. Voor de Minister is het feit dat een leverancier uit Nederland komt een duidelijk positief criterium bij de gunning van aanbestedingen. Zou de Minister willen overwegen dit criterium ook aan te houden bij aanbestedingen in het veld van cybersecurity?

De **voorzitter**:
Ogenblik. Er is een interruptie van mevrouw Buitenweg voor u.

Mevrouw **Buitenweg** (GroenLinks):
Ja, ik vind het heel interessant wat collega Laan zegt. Kan zij dat wat meer uitwerken? Ziet zij voor zich dat bij aanbestedingen de voorkeur uitgaat naar een Europese leverancier, zoals ik net ook betoogde? En dat zelfs als een ander systeem meer state of the art is of goedkoper is, het een voorkeur heeft om met die Europese leverancier in zee te gaan? Hoe moet ik dat zien?

Mevrouw **Laan-Geselschap** (VVD):
We kunnen heel concreet kijken naar wat er bij Defensie gebeurt. Er is daar een aanbestedingsprocedure waar nadrukkelijk dit soort elementen

als criterium zwaar wordt meegewogen. Je zou dus kunnen kijken in hoeverre het mogelijk is om dat soort zaken te kopiëren naar deze processen. Je zou dan iets doen wat in Nederland al gebruikelijk is en wat bij een ander ministerie al functioneert. Dus waarom zou je het hier dan niet kunnen doen? Ik zou dat in onderzoekende zin aan de Minister willen vragen en daar eventueel een actie aan willen verbinden.

Mevrouw **Buitenweg** (GroenLinks):
Maar dat is dan in Nederland, hoor ik. Dat is toch best ingewikkeld met die interne markt? Moet dit juist niet Europees gebeuren? De aanbesteding gaat Europees en het belangrijkste is dat die bedrijven in Europa groter worden. Dat kan desnoods ook een bedrijf in Frankrijk zijn, maar in ieder geval niet buiten de Europese Unie.

Mevrouw **Laan-Geselschap** (VVD):
Mijn focus ligt altijd eerst op Nederland. Ik begrijp dat mevrouw Buitenweg altijd wat verder over de grens kijkt, ook gezien haar ervaringen daar. Ik sta er niet negatief tegenover. Het kan een positieve uitbreiding zijn. Ik ben altijd voor Nederland en als Nederland in Europa beter wordt, dan ben ik ook voor Europa. We kunnen uw aanvulling daarop zeker meenemen.

De **voorzitter**:
Dank u wel. Dan is er ook op dit punt nog een interruptie van de heer Verhoeven.

De heer **Verhoeven** (D66):
Ja. Hoe belangrijk is het voor de VVD dat er concrete feiten zijn met betrekking tot de veiligheid van systemen, bij C2000 maar ook bij 5G, versus waarschuwingen en risicoanalyses? Daarnaar ben ik op zoek. Ik categoriseer de waarschuwingen van de AIVD toch vooral in de categorie risicoanalyses. Terwijl het lastig is om harde feiten te vinden op basis waarvan een bepaald bedrijf een gevaar zou zijn voor Nederland. Hoe ziet de VVD dat?

Mevrouw **Laan-Geselschap** (VVD):
Ik ben geen techneut. Ik suggereer ook helemaal niet dat ik in die zin de kennis in pacht heb. Als VVD'er – dat stuk heb ik overgeslagen omdat we maar vier minuten hebben – gaan wij altijd uit van het fenomeen nationale veiligheid. Wat is het risico voor onze veiligheid? Dat staat voor ons centraal. Als er diensten zijn die echt verstand van zaken hebben en zeggen dat iets een risico is, kijken wij daar serieus naar. Iedereen kan als belangenbehartiger bij ons aan tafel schuiven om uit te leggen waarom die risico's in zijn of haar ogen minder groot zijn. Dat is zeer terecht en daar ben ik ook groot voorstander van. Maar die uitleg moet altijd worden afgewogen door een neutraal persoon, in dit geval zijnde de dienst.

De heer **Verhoeven** (D66):
Ik ben ook geen techneut en ik ben ook niet op zoek naar iets anders dan wat ik vroeg. Ik wil een algemener punt aansnijden. Misschien wil de Minister daar straks iets over zeggen. Anders zal ik het hem straks zelf in mijn inbreng vragen. In het kader van de nationale veiligheid kunnen bepaalde organisaties zoals diensten altijd uitspraken doen en vervolgens zeggen: we kunnen verder niet op details ingaan, maar er is echt sprake van een verhoogd risico, een substantiële dreiging, een reëel gevaar. Wij luisteren dan natuurlijk serieus naar die organisaties. Tegelijkertijd zie ik steeds meer in stukken van bedrijven dat er feitelijk nog nooit iets is aangetoond. Daar ben ik ook niet geheel ongevoelig voor. Ik zoek naar de manier waarop we daarmee met elkaar moeten omgaan in deze Kamer.

Anders kun je altijd blind varen op de woorden «nationale veiligheid», want er is nou eenmaal een risico.

Mevrouw **Laan-Geselschap** (VVD):
De heer Verhoeven stelde de vraag volgens mij indirect aan de Minister, dus daar ben ik dan ook nieuwsgierig naar. Wat ons betreft: bij twijfel, niet inhalen.

De **voorzitter**:
Voordat u begint – u bent zich bewust van de tijd, dat is heel duidelijk – u heeft nog een minuut. Ik heb mevrouw Buitenweg wat extra tijd gegeven, dus die geef ik u ook. Dat halen we wel weg bij de Minister.

Mevrouw **Laan-Geselschap** (VVD):
Dan kan ik iets minder snel praten. Een heel ander punt dan, dat toch weer aansluit bij de woorden van mijn voorgangster, maar op een andere manier. De aanslagpleger van de kerstmarkt in Berlijn is uiteindelijk opgepakt, maar niet voordat hij eerst door vijf verschillende Europese landen kon reizen. Op dit moment zijn er allerlei nieuwe technologieën die iets dergelijks zouden kunnen voorkomen; biometrische camera's zijn hier een voorbeeld van. Kan de Minister aangeven of er nagedacht wordt om een dergelijk systeem in Nederland te gaan gebruiken, bijvoorbeeld bij grensovergangen of bij ov-knooppunten en dergelijke? Maar alleen dan als er een dreiging is voor de nationale veiligheid. Wij pleiten zeker niet voor het Chinese systeem. Nadat ik vroeger 1984 en Brave New World heb gelezen, krijg ik dat horrorbeeld nooit meer van mijn netvlies.
Het gebruik van bigdata-analyses biedt op het gebied van antiterrorisme ook nog heel erg veel mogelijkheden. Kan de Minister ons daarvan op de hoogte houden? Hoe loopt dat? Welke organisaties in Nederland zijn daarbij betrokken? Wat is de voortgang? Daarbij wil ik nogmaals nadrukkelijk aangeven dat wij in Nederland heel veel kunnen en ook zouden moeten doen met de kennis en kunde die wij in huis hebben.
Dank u wel, voorzitter.

De **voorzitter**:
Ik dank u zeer. Dan is het woord aan de heer Verhoeven van D66.

De heer **Verhoeven** (D66):
Ja, voorzitter. Razend interessant allemaal. Ik ben het zeer eens met de opmerkingen van mevrouw Buitenweg. Aan de ene kant is mijn antwoord als D66 dat we terughoudend moeten zijn met allerlei vormen van surveillance als we niet weten wat daarvan de gevolgen zijn. Het tweede is dat we inderdaad vooruitstrevend moeten zijn met het neerzetten van een Europese techindustrie. Dat is nu eenmaal het gevolg van de nieuwe verhoudingen in de wereld. Zelfs de wat meer protectionistische benadering die doorklinkt in de woorden van de beide collega's, begrijp ik wel. Maar we hebben te maken met een nieuwe werkelijkheid.
Ik ben vooral bij dit AO aanwezig, omdat ik graag een debat wilde voeren over de nationale veiligheid en het Cybersecuritybeeld Nederland 2019. Dat is nu alsnog aan de agenda toegevoegd, waarvoor dank. In dat stuk stond bijvoorbeeld, ik citeer: «Ontwrichting van de maatschappij ligt op de loer. Vanwege de omvang van de dreiging ontstaan er risico's voor de nationale veiligheid.» Een ander citaat: «Voorbereidingshandelingen voor verstoring en sabotage vormen een potentiële dreiging voor de onafhankelijkheid en zelfstandigheid van Nederland.» Dat zijn echt hele stevige woorden van een zeer serieuze organisatie, de NCTV, die dat Cybersecuritybeeld uitbrengt. Het ligt in de trend van de voorgaande jaren, maar het wordt wel steeds meer. Dat geeft toch een gevoel van onrust. Het lijkt alsof er op de een of andere manier iets aan de hand is waar we niet genoeg mee doen. Ik heb drie voorstellen die ik aan de Minister wil

voorhouden. Allereerst een scan van kwetsbaarheden. Dit ligt een beetje in het verlengde van wat de Minister in zijn eigen stuk een breed publiek-privaat oefen- en testprogramma noemt. Het Nederlandse bedrijf KPN heeft al eerder gepleit voor een programma waarin de vitale infrastructuur op kwetsbaarheden wordt gescand om die vervolgens te dichten. Is de Minister bereid om zo'n publiek-privaat programma op te zetten of in gang te zetten?
Het tweede punt gaat over ethische hackers. Dat zijn hackers die de overheid of andere bedrijven helpen om kwetsbaarheden te vinden en te dichten, zodat ze niet in handen van kwaadwillenden vallen. Is de Minister bereid om een actievere rol voor ethische hackers in te ruimen bij dit probleem, bijvoorbeeld via een bedrijf als HackerOne?
De NCTV wijst heel sterk op attributie, het kunnen aanwijzen van een aanvaller en de dader proberen te identificeren. Dat is lastiger bij digitale aanvallen. Daar ligt een probleem en daar wijst de NCTV ook op. Het wordt steeds moeilijker omdat capaciteit een probleem is en het gevaar van onjuiste of politiek gemotiveerde attributie is sowieso steeds groter, waardoor iemand onterecht kan worden beschuldigd, wat de zaak alleen maar zwakker maakt. Een internationale organisatie voor de attributie van cyberaanvallen zou kunnen helpen, vergelijkbaar met de OPCW die dat doet op het gebied van chemische wapens. Is de Minister bereid om daarnaar te kijken en daarvoor te gaan pleiten in Europees verband? Sowieso denk ik dat er heel veel op Europees niveau zou moeten gebeuren op dit gebied.
Hoelang heb ik nog, voorzitter?

De **voorzitter**:
Een interruptie van mevrouw Buitenweg. U heeft nog een minuut.

Mevrouw **Buitenweg** (GroenLinks):
Misschien help ik u hiermee juist, zodat u er nog iets over kan vertellen. Ik vind het op zich een heel interessant idee om daarin gezamenlijk op te trekken en kennis te delen om dat te kunnen doen. Tegelijkertijd gaat het niet alleen maar om technische kennis, maar ook om veel intelligence van de veiligheidsdiensten. Het blijft heel erg ingewikkeld om daar heel goed op samen te werken. Aan de ene kant willen we daar meer Europees op samenwerken, aan de andere kant zie je dat er ook binnen Europa landen zijn waarmee niet wordt samengewerkt. We delen bijvoorbeeld niet eens informatie met Oostenrijk op dit moment. Dus, hoe reëel is het dat we juist die sensitieve data ook gaan delen?

De heer **Verhoeven** (D66):
Terecht punt. Ik denk dat er een aantal spanningsvelden zijn waarbij het de hele tijd een beetje zoeken is naar een werkbare balans. Over het eerste spanningsveld hadden we het net al; dat zijn de nieuwe verhoudingen in de wereld. Hoe ver ga je in het beschermen van mensen op het gebied van veiligheid waardoor je de privacy van een burger schendt? Een ander spanningsveld is in hoeverre je je open economie moet afgrendelen, omdat er andere bedrijven of werelddelen zijn die machtig zijn. Dit is dus een derde voorbeeld van een spanningsveld. In hoeverre moet je gevoelige data uitwisselen binnen Europa, terwijl er ook landen zijn die hele andere standaarden hebben dan wij op het gebied van bijvoorbeeld het vergaren van die data en het beschermen van privacy van burgers? Daar is terughoudendheid ook weer nodig. Aan de andere kant, we hebben gezien dat het uitwisselen van data tussen de verschillende diensten tot concrete voorkoming van aanvallen heeft geleid. Wat mij betreft zou er een Europese controle op moeten kunnen zijn. Die is er nu niet omdat de uitwisseling nu plaatsvindt tussen landen en er wel controle op de diensten door de landen zelf is. Dus wat mij betreft zou je naar een

Europees niveau van controle moeten, om te kijken of de uitwisseling van data binnen de grenzen van het burgerrecht valt.

Mevrouw **Buitenweg** (GroenLinks):
Ik snap dat heel goed als een beeld heel ver weg. Tegelijkertijd, van Oostenrijk wordt nu gezegd dat de veiligheidsdiensten te veel gelieerd waren aan de Russen, en er zijn een aantal landen die geen rechtsstaat zijn. Los daarvan is er nog een ander probleem. Als op een gegeven moment een attributie heeft plaatsgevonden – «het is waarschijnlijk dat land» – zit daar een enorme politieke verantwoordelijkheid aan vast. Dat heeft grote diplomatieke gevolgen. Dat is mijn zoektocht, terwijl ik het idee steun om het als land niet allemaal alleen te moeten doen. Het is juist een Europese kwestie; daar ben ik het mee eens. Tegelijkertijd vraag ik me af waar de politieke verantwoordelijkheid ligt, als je een soort technische organisatie hebt opgetuigd die juist zo'n politiek besluit moet nemen.

De heer **Verhoeven** (D66):
Overigens werkte niet de veiligheidsdienst van Oostenrijk samen met de Russen, maar een van de regeringspartijen in Oostenrijk zou banden hebben met de Russen.

Mevrouw **Buitenweg** (GroenLinks):
Maar onze AIVD heeft geweigerd informatie over te dragen aan Oostenrijk, vanwege die banden.

De heer **Verhoeven** (D66):
Zeker. Absoluut. Die afweging is inderdaad gemaakt. En het feit dat die afweging is gemaakt, geeft weer aan dat er door onze diensten goed wordt nagedacht over wat je wel of niet doet. Dat is een van de bezorgdheden die u ook vaak geuit heeft. Ik vond dit een verontrustend bericht omdat dit in Europa speelt. Ik vind het goed dat Nederland er zo mee omgaat. Dit was een beetje hardop nadenken over een dilemma. Ik zal dat ook als antwoord doen en ik zal het kort houden. Ik denk dat het echt zoeken is naar een Europese oplossing, die recht doet aan de hele vergaande positie van Nederland op het gebied van zoeken naar balans tussen veiligheid en burgerbescherming aan de ene kant en privacy en burgerrechten aan de andere kant. Als Nederland moeten we proberen de Europese standaard zodanig hoog te krijgen dat we kunnen toewerken naar een Europees niveau. Dat zou mijn antwoord zijn, maar dat is nog een lange weg.

De **voorzitter**:
Dank u wel. U kunt uw betoog hervatten.

De heer **Verhoeven** (D66):
Zoals mijn bijdrage ook nog een lange weg is, voorzitter.

De **voorzitter**:
Ja, die gaat nog ruim een minuut duren, schat ik zomaar in.

De heer **Verhoeven** (D66):
Zo is het. Ik heb nog een aantal andere punten en de weg eindigt bij meneer Van Dam en mijn tijd tikt door.
De Nationale Veiligheid Strategie heeft aandacht voor de maatschappelijke gevaren van toenemende polarisatie – dit punt staat ook op de agenda – democratische ondermijning en belemmering van grondrechten zoals persvrijheid. Het voorkomen hiervan is een hele grote prioriteit. De Minister schrijft dat hij gaat voor een brede overkoepelende aanpak gericht op de bevordering van samenleven. Dat is een beetje vage benadering. Wat bedoelt hij met «bevordering van samenleven»? Wat

gaat de Minister concreet doen om de ondermijning en belemmering van grondrechten zoals persvrijheid te bestrijden?
Een tweede punt is dat hij zegt dat polarisatie communicatie heel belangrijk maakt. Wat doet de Minister om mensen te bereiken die minder goed bereikbaar zijn, zoals mensen die geen Nederlands spreken, laaggeletterd zijn of vanwege hun leeftijd, afkomst of persoonlijke situatie niet in staat zijn om volwaardig mee te doen met de samenleving?
Tot slot een punt over de internationale rechtsorde. In hoeverre sluit onze Nationale Veiligheid Strategie aan op die van onze buurlanden en van de EU Ik hoorde hier naast mij heel terecht «Monica» zeggen. Dat is mevrouw Den Boer. En ik stel deze vraag inderdaad zoals mevrouw Den Boer deze altijd stelt, want zij zou hier eigenlijk hebben moeten zitten.
Dan kom ik bij mijn laatste vraag. Is de Minister het met D66 eens dat juist bij grensoverschrijdende zaken zoals terrorisme, cyberspionage en ondermijning een gezamenlijke aanpak in Europa – we hadden het hier net al over – de beste weg is en er dus afstemming tussen de verschillende lidstaten nodig is, met inachtneming van het dilemma dat mevrouw Buitenweg zojuist op mijn bordje gooide?
Dank u wel.

De **voorzitter**:
Ik dank u zeer. Zo komen we bij de heer Van Dam van het CDA.

De heer **Van Dam** (CDA):
Dank u wel, voorzitter. Excuses dat ik iets later binnenkwam, maar dat heeft te maken met deze laatste weken voor het reces waarin ik aan een vorm van multitasking moet doen, die mij niet per definitie gegeven is.
Ik heb een paar dingen die volgens mij ook al zijn aangeroerd door de collega's, dus ik kan sommige dingen kort houden. In de eerste plaats de polarisatie, het punt waar ook de heer Verhoeven het over had. Dat staat genoemd in het rapport Op weg naar een weerbare open samenleving. Als ik het goed begrijp, is dat rapport een van de bouwstenen geweest die aan de Nationale Veiligheid Strategie hebben bijgedragen. In de Nationale Veiligheid Strategie staat een aantal thema's genoemd: statelijke dreigingen, bescherming vitale infrastructuur, terrorisme. Dan zie ik al allerlei mensen in het hoge geweldsspectrum of met van alles en nog wat op ons afkruipen, terwijl dat punt van polarisatie ook heel erg kan zitten in discussies rond asiel- en migratiebeleid. Dit wordt ook in dat rapport gezegd. De polarisatie is precies ook een heel erg maatschappelijk thema. Wij zijn verworden tot een samenleving waar vooral de uitersten hun mond opendoen, waarvoor heel veel ruimte is, in media, op Twitter en noem alles maar op. Dat terwijl het zo belangrijk is dat het goede gesprek in het midden gevoerd wordt, waarbij je van mening met elkaar kunt verschillen, maar wat niet meteen wil zeggen dat je elkaar de hersens inslaat. In dat opzicht heb ik een vraag aan de Minister, die een beetje in lijn is met de opmerking van de heer Verhoeven. Kan de Minister aangeven hoe niet alleen hij, maar het hele kabinet – want ik denk dat dit een activiteit is die op vele terreinen vorm moet krijgen – met elkaar de polarisatie in de samenleving gaat aanpakken?
Het tweede punt gaat over de WAS-palen. Wat een woord zeg! En wat een, in zekere zin, licht banaal onderwerp breng ik hier naar voren, in vergelijking met de hoogdravende onderwerpen die op de agenda staan. Maar dan nog. Mijn moeder van 86 heeft geen mobiele telefoon. Als er een crisis is, hecht ik eraan dat ook zij op de een of andere manier gewaarschuwd wordt voor wat er gaande is. Wat doen we met onze toeristen in Nederland? Wat doen we als je 's nachts dat ding gewoon uitzet? Ik heb begrepen dat mevrouw Laan daarvoor ook aandacht heeft gevraagd. De Minister heeft gezegd dat hij het een tijdje uitstelt, maar wat het CDA betreft, worden de WAS-palen helemaal niet afgeschaft of regionaal belegd. Een beetje wijzer geworden door de inzichten de laatste

tijd over de kwetsbaarheden op het vlak van de digitale samenleving, vinden wij dat we heel serieus moeten kijken of we die WAS-palen niet veel langer landelijk in stand moeten houden. Graag een reactie van de Minister hierop.
Tot slot, en dat is een beetje een vreemde eend in de bijt van deze agenda, de hele voortgang over de cybercrime-aanpak. Die is een beetje met de haren bij dit AO Nationale veiligheid gesleept. Ik meen door mijn buurman.

De **voorzitter**:
Punt van orde van de heer Verhoeven.

De heer **Verhoeven** (D66):
De heer Van Dam doet nu net of ik iets er met de haren bij heb gesleept. Ik had hier zelfs een apart debat over gewild. Ik heb dat keurig netjes volgens de procedures aangevraagd. Een Kamermeerderheid zei toen: laat meneer Verhoeven nou eens een keer verstandig zijn en geen debat aanvragen; we doen het bij het AO Nationale veiligheid. Toen was het mijn collega Laan die zei: nou, dat is niet slim van je, Kees. Maar meneer Van Dam was een van de suggesteerders van deze oplossing en ik heb naar hem geluisterd. Dus elke beschuldiging aan mijn adres is eigenlijk een beschuldiging aan hemzelf.

De **voorzitter**:
Ik stel voor om kort te schorsen om dit even uit te vechten.

De heer **Verhoeven** (D66):
Ja, dat moet echt uit de weg. Dit kan zo niet langer.

De **voorzitter**:
De heer Van Dam, het woord is aan u.

De heer **Van Dam** (CDA):
Ik denk dat ik me hier wat door de lengte van de haren heb laten leiden, want die zijn bij de heer Verhoeven langer dan bij mij. Ik vrees dat de weergave van de werkelijkheid wel correct door hem is weergegeven. Dat laat onverlet dat dit onderwerp inderdaad bijna een eigen debat rechtvaardigt en er een beetje vreemd bij staat.
Ik pik er één ding uit. We hebben in Nederland een NCSC voor de vitale kant. We hebben ook een DTC – ik moet natuurlijk niet in afkortingen praten; DTC is het Digital Trust Center – dat is voor het mkb, als ik het zo mag zeggen. Mijn vraag is: wat hebben we voor de gewone burger? In België bestaat het Centrum voor Cybersecurity. Dat is een gecentraliseerd platform waarop niet alleen de vitale sector en de andere sectoren zitten, maar waartoe vooral de burger, maar ook scholengemeenschappen, huishoudens en de decentrale overheden zich kunnen wenden voor advies, handelingsperspectief en een antwoord op de vraag wat te doen tegen verschillende vormen van cybercrime. Ik vind dat de burger er nog een beetje bekaaid afkomt in de hele aanpak van cybercrime, ook in preventieve zin. Graag een reactie van de Minister hierop. Hoe staat hij de burger bij? Heel veel burgers gaan niet naar de politie als hun iets overkomt, nee, die gaan naar hun detailhandelaar toe – voor zover ze die nog hebben – om te vragen wat ze nou moeten doen. Dus ik zou graag meer tekst willen over het handelingsperspectief voor de burger in preventieve en repressieve zin als het gaat om cybercrime.
Dank u wel.

De **voorzitter**:
Ik dank u zeer. De Minister heeft verzocht om een kwartiertje. Dan schors ik de vergadering in ieder geval tot 13.20 uur. Is dat ook het moment dat we gaan stemmen?

De heer **Van Dam** (CDA):
Mag ik een puntje van orde maken? Ik moet niet alleen stemmen, ik heb ook in de regeling iets op de agenda staan. Mevrouw Laan ook, hoor ik net. Hoe eerder we door kunnen gaan en hoe korter we het kunnen maken, graag.

Minister **Grapperhaus**:
Ik wil best kijken. Er zijn enkele dingen die ik werkendeweg misschien al kan beantwoorden. Ik kan al wel aan de slag gaan met een aantal dingen.

De **voorzitter**:
Ik stel voor dat we schorsen tot de heer Van Dam in ieder geval klaar is bij de regeling.

Minister **Grapperhaus**:
Laten we tien minuten schorsen. Dan gaan we over tien minuten door en zodra u weg moet, moet u weg. Is dat een goed idee?

De **voorzitter**:
Helemaal goed. Dan schors ik tot 13.17 uur.

De vergadering wordt van 13.07 uur tot 13.21 uur geschorst.

De **voorzitter**:
Het woord is aan de Minister van Justitie en Veiligheid.

Minister **Grapperhaus**:
Voorzitter. Ik begin mijn overleg met toch even een opmerking te maken die verband houdt met de ramp rondom de MH17. Laat ik beginnen met nogmaals mijn medeleven te betuigen richting de nabestaanden, die al bijna vijf jaar leven met de gevolgen van die afgrijselijke gebeurtenis. Voor hen was gisteren toch weer een heel belangrijk moment. Ik zeg dat niet zomaar, maar ook in het licht van dit algemeen overleg. Want zoals ik in de brief Tegengaan statelijke dreigingen heb gemeld, is een van de uitingsvormen van statelijke dreiging desinformatie. In het licht van die dreiging wil ik even ingaan op de persconferentie van het Joint Investigation Team en het Openbaar Ministerie van gisteren. U weet wat er tijdens die persconferentie is bekendgemaakt: er wordt een aantal verdachten vervolgd en maart volgend jaar is de eerste zitting. Het is in het kader van dit AO belangrijk om ook te spreken over de rol die desinformatie speelt rondom MH17.
Kort na de gebeurtenissen was er sprake van veel verschillende theorieën over de toedracht van de ramp. Veel van die theorieën zijn inmiddels onjuist gebleken. In sommige gevallen bleken ze bewust gecreëerd te zijn om verwarring te scheppen. Die desinformatie rondom het onderwerp MH17 zien we tot op de dag van vandaag. Ik verwijs naar de jaarverslagen van de inlichtingendiensten, maar ook naar diverse media. Bijvoorbeeld NRC Handelsblad publiceerde daarover in samenwerking met de Universiteit van Amsterdam en De Groene Amsterdammer in mei jongstleden een aantal lezenswaardige, heldere artikelen. Het is van groot belang om ons goed voor te bereiden op desinformatie in aanloop naar en tijdens het strafproces. De desinformatie kan gericht zijn op het proces en de instituties die daarbij betrokken zijn. U kunt dan denken aan instituties als onze democratische rechtsorde of de rechtspraak in algemene zin. Maar ook de rechtbank Den Haag of het Openbaar

Ministerie in het bijzonder kunnen het slachtoffer worden van desinformatiecampagnes. Dat alles is bedoeld om het strafproces negatief te beïnvloeden en ons vertrouwen in de onafhankelijke rechtspraak te ondermijnen. Desinformatie kan ook gericht zijn op individuen in het bijzonder. Die is dan bedoeld om personen die betrokken zijn bij het strafproces in diskrediet te brengen en zo de geloofwaardigheid van de rechtspraak negatief te beïnvloeden.
Zoals u weet, hebben wij geen Ministerie van Informatie dat kan bepalen hoe het in elkaar zou moeten zitten. In onze democratische rechtsorde bepaalt de staat niet wat de waarheid is. Die belangrijke taak wordt in samenspraak tussen burgers, media en wetenschap uitgevoerd. De rechtspraak heeft er een belangrijke rol in, daar waar wij als regering ons uiteraard zeer terughoudend opstellen.
Het is evengoed van belang dat we allemaal bewust moeten zijn en blijven van desinformatie en de verstorende werking daarvan op onze samenleving. Het is ook daarom dat de rijksoverheid op 11 maart jongstleden een bewustwordingscampagne is gestart over desinformatie. Ik wil iedereen op het hart drukken dat als er onduidelijkheid bestaat over informatie, over het strafproces inzake MH17 of over zaken die daarmee te maken hebben, het essentieel is om altijd navraag te doen bij de relevante organisaties zelf. Zij vervullen immers allemaal een eigen rol en hebben een eigen verantwoordelijkheid binnen onze onafhankelijke en onpartijdige rechtspraak. Zij kunnen verantwoording afleggen, vragen beantwoorden en feiten geven, zodat we allemaal minder vatbaar zijn voor desinformatie en de effecten hiervan.
Voorzitter, u wilt mij deze misschien wat lange en zware verklaring vergeven. Gezien het grote belang van het MH17-proces en dat er gerechtigheid komt, acht het kabinet het noodzakelijk dit nog eens uitdrukkelijk in het kader van dit algemeen overleg onder de aandacht te brengen.

De **voorzitter**:
Dat spreekt vanzelf.

Minister **Grapperhaus**:
Ik ga nu verder met de beantwoording.

De **voorzitter**:
U gaat nu verder met de beantwoording van de inbrengen.

Minister **Grapperhaus**:
Voorzitter. Een van uw leden zei het terecht: we hebben het vandaag over een behoorlijk scala aan verschillende onderwerpen. Nationale veiligheid is dan ook een groot iets wat in allerlei onderwerpen uiteenvalt en waarbij, zoals de heer Verhoeven zei, ook iets als cybercrime op de agenda kan komen. We spreken vandaag slechts over een aantal van die onderwerpen, maar de veelheid rechtvaardigt dat wij regelmatig met uw Kamer bij elkaar komen. Ik stel het op prijs dat we die, zoals ik weet, kritische gedachtewisseling met elkaar hebben en blijven houden. Wij zijn bij uitstek een democratische rechtsstaat en dat willen we zo houden. Daarom is de nationale veiligheid voor ons van groot belang.
Ik begin met een onderwerp dat door de heren Van Dam en Verhoeven is aangeroerd en dat enigszins aansluit bij wat ik eerder zei over desinformatie. Dat is de polarisatie. Polarisatie is ongewenst als het tegenstellingen verscherpt en mensen met de ruggen naar elkaar toe zet. Het Sociaal en Cultureel Planbureau wijst in het Continu Onderzoek Burgerperspectieven van het eerste kwartaal van 2019 op zorgen die burgers kunnen hebben over vergrote tegenstellingen en polarisatie. Een van de oorzaken van die zorgen is gelegen in de snel veranderende samenstelling van de bevolking. Diversiteit naar herkomst is in korte tijd een structureel

kenmerk van onze samenleving geworden. Duidelijk is dat als mensen elkaar in de samenleving niet tegenkomen, elkaar niet kennen, een beeld kan ontstaan dat we van elkaar verschillen waardoor vooroordelen, angst en uitsluiting kunnen volgen. Daarom zet het kabinet zich ervoor in dat iedereen kan meedoen.
Naast de inzet van het kabinet op de verduidelijking van de burgerschapsopdracht van primair en secundair onderwijs, het tegengaan van discriminatie, betere inburgering en verdere integratie op de arbeidsmarkt, zal collega Koolmees zich namens het kabinet ook inzetten voor het samenleven in de diverse wijken. Ik verwijs naar de Nationale Veiligheid Strategie, die wel een paar keer in dit overleg kan terugkomen. Dat is een kabinetsstuk waarbij de verschillende departementen hun eigen verantwoordelijkheden oppakken. Dus de discussies daarover moeten bijvoorbeeld ook met SZW, Sociale Zaken en Werkgelegenheid, of OCW, Onderwijs, Cultuur en Wetenschap, gevoerd worden. Deze Minister heeft in ieder geval de verantwoordelijkheid om als aanjager te fungeren, om ervoor te zorgen dat die initiatieven van de grond komen en dat de discussie met uw Kamer er ook daadwerkelijk is.
Ik wijs ten slotte nog op de verkenning van de WRR, De nieuwe verscheidenheid. Die laat bij toenemende diversiteit een zwakker ervaren buurtcohesie zien. We hebben in dat kader besloten om met de Vereniging van Nederlandse Gemeenten de gemeenten te gaan ondersteunen bij vraagstukken op het gebied van diversiteit en inclusie. Nogmaals, de rol van het Rijk moet een faciliterende zijn. Er bestaat geen «one size fits all»-aanpak. Je moet dat vooral lokaal met elkaar toespitsen en oppakken.
Ik wilde op de vraag van de heren Van Dam en Verhoeven een aantal voorbeelden geven. Ze formuleerden het beiden ietwat anders, maar het kwam erop neer dat ik het heel breed formuleer en zij zich afvroegen hoe het zich dan toespitst. Het is echt de bedoeling dat wij als Ministers, als bewindslieden, allemaal op onze eigen terreinen de strijd met polarisatie aangaan en daar initiatieven voor ontplooien.

De heer **Van Dam** (CDA):
Ik ben wellicht wat traag, maar ik herkauw nog op het openingsstatement over MH17 en desinformatie van de Minister. Dit is na gisteren het eerste publieke debat dat de Minister voert. Ik wil toch weten of hij deze gelegenheid aangrijpt om dit naar voren te brengen of dat er na gisteren een specifieke aanleiding is. Ik vind namelijk dat de inhoud van wat het JIT gepresenteerd heeft zo formidabel staat, dat ik bij mijzelf denk: wie kan daar met welk verhaal aan tippen of daar iets aan afdoen? Ik heb behoefte om daar iets meer duiding van te hebben.

De **voorzitter**:
Een ogenblik. Voordat we dit gaan doen, kijk ik even naar de andere leden. Ik zie dit vooral als een mededeling en niet als een onderdeel van het debat. U gaat zo meteen bij de regeling zelf een debat aanvragen over gisteren, dus ik wil even kijken of er behoefte is om dit nu te doen. Ik kijk even naar de anderen.

De heer **Verhoeven** (D66):
Ik heb geen enkel bezwaar. Als de Minister in een debat met de Kamer deze hele belangrijke woorden zegt, vind ik dat een Kamerlid daarover een vraag moet kunnen stellen.

De **voorzitter**:
Ik wil het voor de orde toch even vastgesteld hebben.

Mevrouw **Laan-Geselschap** (VVD):
Als het niet te lang duurt, want het is mijn portefeuille niet en ik kan er ook moeilijk op reageren, ook al spreek ik namens de VVD altijd uiteraard uit één mond.

De **voorzitter**:
Dan houden we het heel kort. Dit was even de orde. Uw vraag is gesteld, dus we gaan de Minister horen.

De heer **Van Dam** (CDA):
Meer dan een duiding waarom de Minister dit nu naar voren brengt, hoeft voor mij niet.

De **voorzitter**:
Prima.

Minister **Grapperhaus**:
Laat ik beginnen te zeggen dat die duiding gebaseerd is op de vaststelling van de NCTV, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, dat er eerder sprake was van desinformatie. En niet een klein beetje, maar echt in aanzienlijke mate. Ik heb dat eerder genoemd. Het is echt een belangrijk, groot proces waarbij een aantal landen heeft samengewerkt in het Joint Investigation Team. Daarbij werken we onder – ik zou haast willen zeggen «onder de hoede van» – de VN-resolutie die opriep tot onderzoek en berechting van de verantwoordelijken. Dan is het van belang – ik doe dat natuurlijk namens het kabinet – dat ik als Minister van Justitie en Veiligheid mensen er nog eens goed op wijs dat er de komende maanden grote kans bestaat op allerlei vormen van desinformatie om te proberen dat proces te ontwrichten, eigenlijk zoals in het cybersecuritybeeld wordt beschreven hoe die ontwrichting kan plaatsvinden. Ik roep eenieder op om zich niet iets te laten wijsmaken en ervoor te zorgen dat hij zich goed verstaat met de organisaties die bij het proces betrokken zijn, om van hen te horen hoe de feiten liggen. Het proces is van groot belang, net als de gerechtigheid waar nabestaanden recht op hebben en naar op zoek zijn. Ik wil dat graag nog een keer in een separaat debat met uw Kamer uitvoeriger exploreren. Daar heb ik geen enkel bezwaar tegen.

De **voorzitter**:
Is dit afdoende duiding, meneer Van Dam?

De heer **Van Dam** (CDA):
Zeker. Ik wilde alleen checken dat er geen concrete aanleiding was om die opmerking te maken. Dat is nu duidelijk gezegd. Ik heb er alle begrip voor, maar ik wilde daar helderheid over hebben.

Minister **Grapperhaus**:
Er is in de afgelopen jaren voldoende aanleiding geweest om dat hier hardop zo te zeggen.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Misschien is het goed om iets te zeggen rondom C2000 en het onderwerp van de WAS-palen, dat door de heer Van Dam min of meer als knus gekwalificeerd werd, althans de naam daarvan. In antwoord op mevrouw Buitenweg kan ik zeggen dat ik opdracht heb gegeven om tot een verkenning te komen hoe wij het advies van de AIVD om te werken aan een vervanging van dit nieuwe systeem, kunnen overnemen. Zoals ik op

26 april heb geschreven, zal ik uw Kamer na de zomer over die verkenning informeren. Dan gaan wij het traject verder af met elkaar, terwijl tegelijkertijd conform het advies van diezelfde AIVD het nu nieuwe systeem dat daarnaartoe gemigreerd is, in werking gaat.
In antwoord op vragen van mevrouw Buitenweg en mevrouw Laan zeg ik dat het oorspronkelijk de bedoeling was dat het C2000-systeem tien jaar zou meegaan. Zoals gemeld in de brief van 26 april gaan we aan de slag met die verkenning. Het is mogelijk dat het huidige systeem daarom korter dan tien jaar gebruikt zal worden. Dat hangt uiteraard ook af van aan de ene kant die verkenning naar het nieuwe systeem en aan de andere kant de ontwikkelingen op het gebied van offensieve cyberprogramma's in het algemeen en in de toekomst. Het specificeren, de marktverkenningen, de aanbestedingen en de realisatie duren naar alle waarschijnlijkheid rond de vijf jaar. We moeten dat niet precies nemen, maar ik vind wel dat ik de verplichting heb om een indicatie te geven van hoe lang het duurt.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel voor de heldere antwoorden, ook over die beoogde tien jaar en dat we nu kijken of het toch niet korter kan, ook gezien het advies van de AIVD. Ik probeer te begrijpen wat er verkend wordt. Wordt er nou verkend hoe zo'n systeem eruit kan zien, of dat het nodig is? De AIVD zegt dat het nodig is en de Minister zegt dat hij het advies overneemt. Kan hij iets duidelijker zijn over wat hij aan het verkennen is?

Minister **Grapperhaus**:
Ik verken hoe we gaan insteken op het initiëren van een heel nieuw proces van specificatie, marktverkenning, aanbesteding en tenslotte realisatie van een nieuw nieuw systeem. Ik noem het maar even zo voor de kijkers thuis, omdat ze het anders kwijtraken. We migreren op afzienbare termijn naar het nieuwe systeem. Een aantal deskundige instanties, de AIVD, Xebia, professor Jacobs en andere, hebben gezegd dat daarbij een aantal veiligheidsrisico's in beeld zijn. Die zijn geadresseerd en er worden maatregelen genomen. De AIVD zegt echter dat ik moet toewerken naar een nieuw nieuw systeem en dat de periode korter wordt dan tien jaar. Dan kom ik meteen op het punt dat dat een kostenraming met zich meebrengt. Daarop kom ik uiteraard bij uw Kamer terug. Samenvattend is mijn antwoord aan mevrouw Buitenweg: het uitgangspunt is dat we in het kader van het advies van de AIVD en de Nationale Veiligheid Strategie verkennen hoe we het traject van specificatie, aanbesteding en vervolgens realisatie inzetten na de zomer.

Mevrouw **Buitenweg** (GroenLinks):
Dat is helder. We gaan dus nu al kijken naar het vervangen van het nieuwe C2000. Als we kijken hoe dat zo goed mogelijk gedaan moet worden in de toekomst, kan ik mij voorstellen dat het enige jaren duurt. Het duurde ook lange tijd voor het komende C2000 er kwam. Gaan we uit van een bepaalde tijd waarin we per se dat C2000 moeten hebben of gaan we nu zo snel als kan het huidige C2000 vervangen en zal dat een paar jaar duren?

Minister **Grapperhaus**:
We geven in de verkenning aan hoe we een nieuw systeem gaan ontwikkelen, en op een gegeven moment realiseren en in werking zetten. Daarom noem ik het steeds een «nieuw nieuw systeem». Er komt dan echt een nieuw nieuw systeem. Een belangrijk punt is hoe we de invloed van statelijke actoren bij dat nieuwe nieuwe systeem tot nul brengen. Dat wordt absoluut een van de hoofdpunten. Ik zeg toe dat ik na de zomer bij u terugkom op de verkenning van wat het traject ongeveer inhoudt. Dan heeft u een driedimensionaal beeld van hoe enerzijds het nieuwe systeem

met alle veiligheidswaarborgen die de AIVD heeft geadviseerd aan de gang gaat en anderzijds hoe wij met de ontwikkelingen van het nieuwe systeem omgaan. Nogmaals: het tijdsbestek om dat hele traject af te leggen, schatten wij in op vijf jaar. Dat is de helft van de tien jaar die oorspronkelijk begroot was, dus er is zeker een kostenaspect op het punt van de afschrijving van de levensduur van het nieuwe systeem, niet te verwarren met het nieuwe nieuwe systeem. Het nieuwe systeem gaan we dus sneller afschrijven.

De **voorzitter**:
Het oude nieuwe systeem.

Minister **Grapperhaus**:
Het oude nieuwe systeem hebben we nog niet in kaart gebracht.

De **voorzitter**:
Volgens mij is het antwoord helder, als ik zo naar mevrouw Buitenweg kijk. Ik vraag u verder te gaan met uw beantwoording.

Minister **Grapperhaus**:
Dan de zogeheten WAS-palen. Het zijn WAS-palen, maar ze zijn er nog steeds. Ze hebben wel degelijk een belangrijke betekenis gehad, maar al in 2014 is door mijn voor-voorganger geconstateerd dat het systeem van de WAS-palen in een aantal opzichten niet meer optimaal voldeed aan het doel waarvoor het was bedoeld. Dat is een zo groot mogelijk bereik in het geval van een crisissituatie. Laat ik meteen maar zeggen dat het bereik van NL-Alert hoog is. Het directe bereik is al 78%. Dat is nog zonder het indirecte bereik doordat mensen elkaar waarschuwen of doordat er bijvoorbeeld waarschuwingsborden of andere dingen zijn. De landelijke dekking van NL-Alert is bovendien veel groter dan die van het WAS-systeem. Sirenes worden op dit moment bij incidenten nauwelijks meer gebruikt door veiligheidsregio's, want als zich een regionaal incident voordoet, wordt NL-Alert ingezet. Sirenes hebben door de komst van nieuwe crisiscommunicatiemiddelen zoals NL-Alert een beperkte operationele inzetwaarde en hebben daardoor nog maar weinig toegevoegde waarde.
Een heel belangrijk extra verschil tussen de WAS-palen, die dat sirenegeluid geven, en NL-Alert is dat NL-Alert een handelingsperspectief biedt. In een NL-Alert-boodschap die u op uw mobiele telefoon krijgt, kan staan dat u naar binnen moet gaan en de ramen moet dichtdoen of dat u moet zorgen dat u niet in een voertuig bent of weet ik veel wat voor handelingsperspectief. Zo'n sirene kan dat moeilijk na het sirenegeluid omroepen. Dat is een heel belangrijk verschil. Dat neemt niet weg dat het punt van mevrouw Laan over de dekking zeer terecht is. Dat is ook de reden dat een aantal kwesties met betrekking tot de dekking geregeld moeten worden. Een voorbeeld is de roaming in grensgebieden waardoor je op je mobiele telefoon, als je vlak bij de grens tussen Limburg en België bent, een signaal hebt van een Belgische provider. Dat is natuurlijk niet best, want dan krijg je geen NL-Alert; dat loopt via de Nederlandse provider. We zijn inmiddels heel ver met het vinden van een oplossing. Een ander voorbeeld betreft speciale middelen voor mensen die niet gewend zijn aan het gebruik van een mobiele telefoon. Ik wil die dingen echt optimaal opgelost hebben. Daarom heb ik in maart gezegd dat ik het verstandiger vind om in plaats van op de aanvankelijk voorziene datum van 1 januari 2020 op 1 januari 2021 definitief over te gaan op NL-Alert. Ten slotte wil ik zeggen dat het aantal mensen dat de NL-Alert-boodschap ontvangt nog steeds stijgt. Bij het begin van mijn ministerschap in december was het 10,3 miljoen. Het gaat elk halfjaar omhoog. Onlangs, in juni, was het 11,6 miljoen. Dan heb ik het over het directe bereik van de boodschap. We komen hierover nog met uw Kamer te spreken, want er is

een motie-Wolbert die heeft gezegd dat alvorens ik definitief de schakelaar omzet – eigenlijk zet ik dan de sirenes uit – langskom bij de Kamer.

Mevrouw **Laan-Geselschap** (VVD):
Dank voor deze analyse van de Minister over de sirenes. Eigenlijk is alles wat hij zegt bekend. We weten allemaal dat er gaten zijn en wat er gebeurt als je in het grensgebied bent. Daar zijn tegenwoordig apps voor en ik hoor graag van de Minister hoe hij daarmee omgaat. Als er nu iets misgaat in Limburg of in het Rijnmondgebied en je buiten op straat loopt of fietst – van een van uw collega's mag dat niet meer met een telefoon in je hand, waar ik overigens groot voorstander van ben – hoor je wel de sirenes. Die waren vroeger in Nederland afdoende, dus in mijn ogen heb ik nog steeds niet van de Minister gehoord waarom en-en voor de Nederlander, voor de nationale veiligheid, niet de beste oplossing is.

Minister **Grapperhaus**:
Dat heeft te maken met het feit dat je voor alle helderheid voor iedereen naar één systeem moet overgaan, plus het feit – ik heb het net uiteengezet – dat NL-Alert veel scherper regionaal ingezet kan worden. Dat is de afgelopen jaren al een aantal keer gebeurd. Bovendien kun je er, of je het nou regionaal of landelijk doet, een handelingsperspectief in zetten. Laat ik vooropstellen dat ik heel goed begrijp dat mensen zeggen: kunnen we niet gewoon die sirenes nog laten loeien? We maken echter op enig moment een overstap naar een nieuw systeem dat een heel groot aantal voordelen heeft. Dat doen we met meer dingen in de samenleving. Als we dit twintig jaar geleden hadden gedaan, was het geen enorm succes geworden, want de mobiele dekking in Nederland was toen natuurlijk veel en veel lager, zowel qua providers als gebruikers. Ergens begin 2020 komen we er zeker op terug. We komen bij de Kamer terug als het definitief een jaar daarna gaat gebeuren.

Mevrouw **Laan-Geselschap** (VVD):
Dat regionale hebben we inderdaad gemerkt: als er iets in Friesland gebeurt, krijgen mensen tot ver in Utrecht via NL-Alert vijftien keer berichten binnen. Daar valt echt nog wel het een en ander aan af te doen. Ik zie ook dat de toekomst er anders uit gaat zien, maar ik hoor nog steeds van de Minister geen afdoende verhaal waarom en-en niet afdoende is voor Nederland. Daar gaan wij nog wel mee verder.

De **voorzitter**:
Ik heb geen vraag gehoord. Het is meer een constatering. Dus ik ga naar de heer Van Dam.

De heer **Van Dam** (CDA):
Ik dank de Minister voor zijn reactie. Ik snap het: het is in lijn met beslissingen die eerder zijn genomen. Alleen zijn er wel meer thema's waarbij in de loop der jaren de palen wat verzet zijn. In dit geval wellicht de WAS-palen. Als we bijvoorbeeld kijken naar de discussie over C2000 en de andere kijk die wij hebben op bijvoorbeeld de betrokkenheid van bedrijven uit bepaalde landen, dan wenden wij op een gegeven moment de steven en varen we een andere koers. Dat speelt bij mij een rol. De NCTV heeft laatst gewezen op onze afhankelijkheid van bepaalde techgiganten. Dat hele NL-Alert loopt ook via techgiganten. Ik wil in de discussie inbrengen dat sinds 2014 of 2015, toen dat besluit is genomen, de loop der tijd tot nieuwe inzichten heeft geleid. Dat is voor mijn fractie een reden om deze oude schoenen niet weg te gooien. Wil de Minister reageren op de vaststelling dat er in de loop der tijd andere inzichten zijn gekomen over de afhankelijkheid van techniek en de kwetsbaarheid die dat met zich meebrengt?

Minister **Grapperhaus**:
Ik ben wat aarzelend om vandaag de hele trits van argumenten nog eens de revue te laten passeren, omdat ik dan een gesprek voer dat hier al een aantal keren is gevoerd. Ik vind het helemaal niet erg – ik kijk dan vooral naar mevrouw Laan – om nog eens in een brief het hoe en waarom op een rij te zetten waardoor mijn voor-voorganger al in 2015 tot dit besluit is gekomen. Even los van het feit dat ik nou eenmaal de Minister ben en het dus ook mijn besluit is, zie ik echt geen argumenten waarom het anders is geworden. Integendeel: het bereik is groter geworden. Ik kom zo op het punt van de technologie. Even voor de aardigheid: uit onderzoek van de Technische Universiteit Twente blijkt dat 89% van de mensen 's nachts de telefoon aan laat staan. Daardoor is het bereik van NL-Alert in de nacht ongeveer even groot als overdag. Hoe kun je mensen zonder mobiele telefoons bereiken? NL-Alert wordt ook op ov-borden aangekondigd en op reclameborden gepresenteerd. Kortom: er zijn een aantal flankerende maatregelen.
Dan het punt van de technologie. We moeten ons niet vergissen: de WAS-palen zijn ook afhankelijk van technologie, die op allerlei punten misschien wel kwetsbaarder is dan de technologie van NL-Alert. Ik kan niet ontkennen dat een hele boosaardige staat of instantie zou kunnen proberen om al die systemen te saboteren, maar dat gaat net zo goed op voor de WAS-palen.
Ik bied aan – maar het hoeft niet – om uw Kamer nog eens in een brief de overwegingen te geven waarom hiertoe gekomen is en hoe inmiddels de voordelen zich alleen maar gestapeld hebben. Dat doe ik met plezier, want ik sta er echt achter.

De **voorzitter**:
We gaan zo zien of daar behoefte aan is. Eerst is er nog meneer Van Dam.

De heer **Van Dam** (CDA):
Ja, kort in een tweede termijn. Ik heb zelf eens wat rondgebeld in het land, naar burgemeesters. Want het idee is dat de veiligheidsregio's het zelf kunnen doen, als ze dat willen. Ik ben in Limburg uitgekomen, waar men er heel ongelukkig mee is dat men het nu zelf moet gaan doen. Ik ben in Alblasserdam uitgekomen, waar een tankwagen heeft gestaan waar iets misging waardoor het hele land een knijper op zijn neus moest zetten. Daar is men zeer ontevreden dat men zelf die WAS-palen moet onderhouden, omdat zo'n alarmeringsmiddel landelijk uniform is. We krijgen een soort verbrokkeling. Dat is één ding. Of u een brief moet schrijven, laat ik graag aan collega Laan over, omdat zij dit punt in eerste instantie heeft opgeworpen. Een tweede punt is het begrip redundantie. Dat vind ik heel erg belangrijk. Je moet voor meerdere ankers gaan. Dat wilde ik nog even naar voren brengen. Maar ik heb geen nadere vragen aan de Minister.

De **voorzitter**:
Nee, maar de Minister wil wel reageren.

Minister **Grapperhaus**:
Voorzitter, op moeilijke woorden reageer ik altijd. Daar kan ik niks aan doen. Wat die redundantie betreft: het systeem voegt op enig moment niets meer toe naast NL-Alert. De reden dat het systeem met de WAS-palen nu door mij met een jaar verlengd is, is dat ik de burger en het publiek wil laten zien dat de problemen met het bereik ook in bijvoorbeeld de grensregio's zijn opgelost. Dat wil ik echt benadrukken. De roamingsproblematiek en dat soort dingen hebben we opgelost. We hebben het helemaal gemaximaliseerd binnen NL-Alert. Qua bereik en qua werking zijn we nu met NL-Alert al een heel eind voorbij de werking die erachter zit volgens onderzoek van universiteiten. Het spijt me dat ik daar zo naar

verwijs, maar ik heb het natuurlijk niet zelf gedaan. U moet goed begrijpen dat ik hier niet met een soort eigenwijsheid zit, omdat ik er helemaal niets voor zou voelen. Nee, er is natuurlijk een uitgebreid besluitvormingsproces aan voorafgegaan, ook binnen het Veiligheidsberaad, om met elkaar te zeggen dat we definitief richting NL-Alert gaan. Twee dingen nog hierover. Eén: ik wil met alle plezier die afwegingen nog eens op een rij zetten in een brief. Het tweede is: we komen hier hoe dan ook nog over te spreken op het moment dat ik ga zeggen dat we overgaan op NL-Alert. Dan hebben we er sowieso nog een gesprek over.

De **voorzitter**:
Ja. Meneer Verhoeven nog op dit punt?

De heer **Verhoeven** (D66):
Ik luister met veel aandacht naar wat gezegd is. Ik had één hele praktische vraag, maar misschien is het al gezegd. Als je je telefoon 's nachts op stil hebt, wordt dat dan doorbroken door het systeem?

Minister **Grapperhaus**:
NL-Alert breekt daardoorheen. En er is nog een ander ding. Ik wil verder niet in privacy treden, maar de heer Van Dam begon zelf over een familielid. Ook voor mensen die geen mobiele telefoon hebben, is er techniek waarmee NL-Alert naar de vaste telefoon is door te geleiden. Dus dan wordt het pas een probleem als mensen helemaal geen telefoon hebben en helemaal geen buren die ze kunnen waarschuwen. Er is dus over al die mogelijke problemen nagedacht en over hoe je die gaat adresseren.

De **voorzitter**:
Ik wil even constateren of er behoefte is aan de brief die de Minister wel wil toezeggen. Dan moet er wel animo zijn om die te ontvangen. We kijken allemaal even naar mevrouw Laan. Wilt u een brief van de Minister waarin hij dit nog eens uitlegt?

Mevrouw **Laan-Geselschap** (VVD):
Ik wil altijd een brief van de Minister. Daar zit ik al jaren op te wachten!

De **voorzitter**:
Ik heb niet het gevoel dat het een hoge urgentie voor u heeft. Maar misschien toch wel?

Mevrouw **Laan-Geselschap** (VVD):
Als in de brief de overwegingen uit 2014 staan om dit systeem in te voeren, dan zeg ik nee. De wereld is echt veranderd. Maar als erin staat waarom de Minister nog steeds hecht aan het systeem en aan de overwegingen van toen en als de Minister een toelichting wil geven op mijn vraag of het niet en-en kan zijn om de nationale veiligheid van alle Nederlanders te waarborgen, dan wil ik graag een brief. Anders hoef ik hem niet.

De **voorzitter**:
Dan wilt u volgens mij graag een brief. Want ik denk dat het laatste er ook in komt. Ik kijk even naar de Minister.

Minister **Grapperhaus**:
Ja, het wordt, zoals dat heet, een «open brief».

De **voorzitter**:
Oké, die brief komt er dus. Wanneer komt die dan?

Minister **Grapperhaus**:
Ik heb dus niet gezegd een «open-minded brief» maar een «open brief».

De **voorzitter**:
Wanneer verwacht u die brief te kunnen schrijven?

Minister **Grapperhaus**:
In september.

De **voorzitter**:
Oké, september. Dank u wel. Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Er zijn nog een aantal vragen die betrekking hebben op de Nationale Veiligheid Strategie. Die sluit aan bij de aanpak van andere landen. De heer Verhoeven vroeg daarnaar. Er is gebruikgemaakt van vergelijkbare strategieën in vergelijkbare landen. Ik noem ze even: Duitsland, Zweden, het Verenigd Koninkrijk, de Verenigde Staten, Australië, Canada, Frankrijk en België. Wij delen onze strategie ook met hen.
Voorzitter. Ik zal niet uitvoerig ingaan op het punt van de statelijke actoren. Daar heb ik een uitvoerige brief over geschreven en er zijn geen vragen over gesteld.
Ik ga direct door naar Hikvision. Mevrouw Buitenweg heeft daar een aantal belangrijke vragen over gesteld. De NCTV kan niet ingaan op individuele bedrijven. In algemene zin kunnen we vaststellen dat er geen eenduidig pakket aan maatregelen ligt tegen een dreiging zoals die door mevrouw Buitenweg wordt beschreven. Dan moet je echt gerichter naar een bedrijf kijken. De risico's die zijn verbonden aan bijvoorbeeld de inkoop of het gebruik van bepaalde goederen worden door Nederland altijd case by case aan de hand van scherpe, vaste criteria gezien. In de C2000-brief ben ik daar ook uitvoerig op ingegaan. Daarin heb ik onder andere verwezen naar wat ik maar even noem de «brief over de Kaspersky-software» van mei 2018. Ik meen dat het 15 mei 2018 was. Daarin ziet u een aantal algemene uitgangspunten voor toetsing.
Maar dan nog steeds wordt er case by case gekeken. Waarom moet je dat uiteindelijk toch weer case by case zien, ook als je die criteria toepast? Omdat de belangrijkste afweging op enig moment is of je bepaalde risico's helemaal goed kunt definiëren en vervolgens ook beheersen of mitigeren. Dat zal per geval verschillen. Dan krijg je ook het juiste maatwerk. In ieder geval wordt ernaar gekeken of er wetgeving bestaat waarbij het betreffende bedrijf op enigerlei wijze wordt gedwongen om samen te werken met een staat en of die staat zich daarbij richt tegen Nederlandse vitale belangen. U vindt dit uitvoeriger terug in mijn brief over de statelijke actoren van april 2019. Uit mijn hoofd gezegd heb ik daarin bij de letters A tot en met J alle toetsingscriteria uitgewerkt en alle velden waarop dat speelt. Dat komt ook in de C2000-brief in wat compactere zin terug.
Mevrouw Buitenweg vroeg ook of we bereid zijn uw Kamer op de hoogte te houden van bedrijven die op de US Entity List staan of daarop worden gezet. Die lijst is voor iedereen toegankelijk. Het ligt dus niet zo voor de hand dat ik die lijst ga rondsturen. Het zou dan ook eerder een verzoek moeten zijn aan mijn ambtsgenoot van Buitenlandse Zaken. Maar die US Entity List is in het publieke domein.

Mevrouw **Buitenweg** (GroenLinks):
Dat was niet mijn verzoek. Ik kan zelf ook zo'n lijst lezen. Daar had ik een deel van die bedrijven uit gehaald. Het is een beetje teleurstellend dat de Minister het opvallend vindt dat ik die lijst kan lezen, maar ik kan dat echt. Mijn vraag was in hoeverre die producten in Nederland gebruikt worden.

De Minister zegt nu dat we alleen aanslaan bij landen waar wetgeving bestaat die een bedrijf dwingt om te handelen conform de wens van dat land. Dit is een bedrijf dat voor 42% in handen is van de Chinese staat. De eigenaar van dat bedrijf heeft zelf gezegd – ik kan daar allerlei citaten bij geven – dat het moet doen wat gezegd is door de communistische partij. De CEO van dat bedrijf staat dat zelf voor. Het Europese hoofdkantoor van dit bedrijf staat in Hoofddorp. Mijn vraag is niet of er een keer een probleem is met dat er een keer ergens een camera staat. Maar het wordt een probleem als dat uitgebreid uitgerold wordt. Althans, dat vind ik een probleem. Ik wil weten of de Minister dat ook een probleem vindt. Het Verenigd Koninkrijk vindt het een probleem. Daar zijn ze nu aan het praten over het feit dat Hikvision ineens oppopt op allerlei bussen en in ziekenhuizen. Zelfs in Westminster was het aanvankelijk. Vinden wij dat aanvaardbaar? Daar hoor ik de Minister niet over.

Minister **Grapperhaus**:
Ik durf het bijna niet te zeggen, maar ik was nog niet toegekomen aan dat aspect. Ik wil nog wel op een deel van uw verontwaardiging inspelen. Ik zei aan het begin: ik kan niet ingaan op de individuele situatie van een bedrijf. Maar ik heb duidelijk geschetst dat we hele scherpe criteria hanteren voor de toetsing van bedrijven die diensten, goederen of delen van infrastructuur aanbieden. Daarbij maken we een aantal overwegingen, waarvan ik er al eentje heb genoemd.
Laat ik uit mijn hoofd even de basics op een rij zetten. Het eerste waarnaar je kijkt is om wat voor dienst of levering het gaat. Gaat het om wezenlijke technologie? Bij die software van vorig jaar ging het bijvoorbeeld om antivirussoftware die diep in onze systemen kwam of zou kunnen komen. Dan weet je dat je dus een hele scherpe toets moet instellen. Het tweede punt is of de leverancier uit een land komt of daar nauwe banden mee heeft waar de overheid kan beïnvloeden wat je als bedrijf doet. Kan de overheid tegen dat bedrijf zeggen: «u moet nu dit doen»? Vervolgens is het de vraag of dat land gekend is als een statelijke actor. Dat wil zeggen: is het een land dat zich richt op – hoe moet ik het zeggen? – het binnendringen in Nederlandse systemen of Nederlandse belangen. Als het antwoord dan ook ja is, dan is de vraag of we de eventuele risico's die aan zo'n systeem verbonden zijn als we met iemand zaken doen, heel erg beheersbaar kunnen maken of tot in de buurt van nul kunnen terugbrengen. Dat zijn de hoofdcriteria. Die staan in mijn brief van 26 april over C2000. U vindt ze veel uitgewerkter in mijn brief over statelijke actoren van enige weken eerder in april 2019.
Ten slotte wil ik nog iets zeggen over...

De **voorzitter**:
Wacht even. We zijn nog bezig met een interruptie.

Minister **Grapperhaus**:
Ik wilde mevrouw Buitenhof – excuus, Buitenweg – nog iets zeggen. Ik zei «ten slotte» omdat ik...

De **voorzitter**:
We moeten door. Ik wijs er tussendoor even op dat er om 14.30 uur stemmingen zullen zijn. En dan hebben we ook nog de regeling.

Minister **Grapperhaus**:
Ik doe enorm mijn best, voorzitter, maar ik wilde via u tot mevrouw Buitenweg nog iets zeggen over het punt van de gezichtsherkenning en de vraag of we met dat soort technologieën moeten werken. Collega Dekker en ik moeten daar samen over gaan. Ik zeg u toe dat wij daarover in gezamenlijkheid in een brief bij u zullen terugkomen. Hoe moet je tegen dit soort dingen aankijken in het licht van de verhouding tussen aan de

ene kant opsporingsbelangen en dergelijke en aan de andere kant privacy? Ik kan u overigens zeggen dat dergelijke techniek op dit moment nog niet door onze diensten wordt gebruikt.

De **voorzitter**:
Mevrouw Buitenweg, heeft u nog een kort antwoord?

Mevrouw **Buitenweg** (GroenLinks):
Fijn dat er een brief komt. Ik hoor graag van de Minister wanneer die komt, want ik denk dat dit heel erg belangrijk is. Ik maak me er zorgen over dat het op een gegeven moment zo veel is. De Minister zegt: onze diensten gebruiken het nog niet. Daarmee bedoelt hij waarschijnlijk dat de AIVD of de politie het nog niet gebruikt. Maar in het Verenigd Koninkrijk zie je bijvoorbeeld dat publieke instellingen het al heel breed gebruiken, zoals ik al zei, bij ziekenhuizen en bussen en dergelijke. Daardoor staat het netwerk er gewoon al. Daar wil ik zicht op hebben. Gebruiken we misschien hier in de Tweede Kamer Hikvision? Ik weet het niet. Maar ik vind dat we daar zicht op moeten hebben. Want bij de andere criteria – kan een overheid beïnvloeden en betreft het een statelijke actor gericht op Nederlandse belangen? – is het antwoord natuurlijk ja. Ik wil dus echt bekijken op welke wijze die risico's beheersbaar kunnen worden gemaakt. Of moeten we dit gewoon niet willen?

Minister **Grapperhaus**:
Maar dan hebben we het over een ander soort onderwerp. Het wordt hier niet systemisch gebruikt, maar dat ze in een ziekenhuis of in een andere instantie een stukje aanwenden, kan ik hier niet uitsluiten. De principevraag is of je dit soort technologieën moet willen, enerzijds in het licht van het karakter van die technologie en anderzijds in het licht van de partijen die die technologie hebben ontwikkeld, de aandeelhouders van die partijen en wie daar allemaal nog meer achter zitten. Nogmaals, in die brief zullen collega Dekker en ik daarop terugkomen, want de privacycomponent speelt hierbij ook een heel belangrijke rol. Ik wil daar verder niet op vooruitlopen, want dat is zijn portefeuille.

De **voorzitter**:
Heel kort nog, mevrouw Buitenweg. Ik moet streng gaan worden.

Mevrouw **Buitenweg** (GroenLinks):
Een heel kort vraagje. In een van die brieven van de Minister – ik ben vergeten in welke – staat ook dat we een investeringstoets gaan doen. Hoeveel procent van de gezichtsherkenningscamera's zijn op dit moment van Hikvision of van Dahua? Hoeveel procent is dat? Dat maakt natuurlijk uit. Als 30% of 40% van onze markt in die handen is, zijn we sowieso al heel erg kwetsbaar. Daarnaast wil ik graag nog weten wat de datum is voor die brief.

Minister **Grapperhaus**:
Een exacte datum voor die brief geef ik niet, maar ik zeg u toe dat die brief in het eerste deel van het laatste kwartaal van dit jaar komt.

De **voorzitter**:
In september is dat.

Minister **Grapperhaus**:
Oktober zo'n beetje.

De **voorzitter**:
O, het eerste deel van het laatste kwartaal. Excuses. Gaat u verder.

Minister **Grapperhaus**:
Het is oktober of de eerste week van november. Dat is de eerste helft.

De **voorzitter**:
Prima. Dat is een indicatie.

Minister **Grapperhaus**:
En dan nog dat andere punt.

De **voorzitter**:
Die percentages? Dat lijkt me ook iets voor in de brief.

Minister **Grapperhaus**:
Daar zal ik ook in de brief op ingaan. Dat kan ik nu echt niet zeggen.

De **voorzitter**:
Dan is er op hetzelfde punt nog een vraag van mevrouw Laan.

Minister **Grapperhaus**:
De bankrekening van mevrouw Buitenweg komt ook nog.

De **voorzitter**:
De bankrekening van mevrouw Buitenweg komt ook nog. Oké.
Mevrouw Laan, nog op hetzelfde punt?

Mevrouw **Laan-Geselschap** (VVD):
Het intrigeert mij wel. Volgens mij komen wij allemaal dit pand niet in als wij beneden niet door de poortjes lopen. Daar staat een gezichtsherkenningssysteem waardoor wij dit gebouw kunnen betreden. Dus wat het woord «systematisch» betreft: wij zitten allemaal al in zo'n systeem. Daarnaast merkte mijn persoonlijke medewerker op dat hij tegenwoordig bij zijn iPhone ook al inlogt met gezichtsherkenning. Hij doet dat niet meer met zijn duim, maar met zijn gezicht. Het systeem is dus al in Nederland. Nog even los van de vragen van mijn collega over de mogelijkheid dat buitenlandse mogendheden daar gebruik van maken, was de vraag in mijn verhaal de volgende. Wat hebben we al in Nederland en kunnen we voor de nationale veiligheid gebruikmaken van systemen, eventueel van anderen, om iemand op te sporen? De eerste helft van het tweede kwartaal van dit najaar is dan wat mij betreft te laat. Anders zeggen we ten aanzien van dit soort ontwikkelingen over een jaar weer: ja, dan hadden we er eerder mee moeten beginnen.

Minister **Grapperhaus**:
Ik heb gezegd «systemisch gebruik». En ik heb ook gezegd dat hier en daar al zo'n element als wat u net omschrijft gebruikt wordt. Maar de vraag was of wij in het kader van onze diensten systemisch dit soort systemen inzetten. Daar heb ik antwoord op gegeven.
Ik ga nu even terug naar de timing. Ik wil juist in die brief heel afgewogen het aspect meenemen van in hoeverre je dit systemisch kunt inzetten voor de opsporing. Dat heb ik net ook genoemd. Je krijgt dan het punt dat de heer Verhoeven ook noemde: surveillance aan de ene kant, privacy aan de andere kant. Mevrouw Laan kent mij als iemand die graag doorpakt, maar ik denk dat ik realistisch moet zijn en u niet moet beloven dat die brief eerder komt. Mijn inschatting van eind oktober of begin november is echt een reële planning. En ik beloof dat als het eerder lukt, de brief eerder komt.

De **voorzitter**:
Meneer Verhoeven nog?

De heer **Verhoeven** (D66):
Hmm...

De **voorzitter**:
Hij staat altijd bekend om zijn puntige vragen.

De heer **Verhoeven** (D66):
Dat is een hele rare manier om mij te introduceren.

De **voorzitter**:
U staat om nog veel meer dingen bekend, maar dit is er één.

De heer **Verhoeven** (D66):
U kiest er nu zomaar één uit!
Ik ben bijna milder dan mevrouw Laan en dat is best bijzonder. Ik snap wel dat er tijd nodig is voor deze ingewikkelde materie. Maar mijn punt is dat hier sprake is van een nieuwe technologie. Ja, die wordt gebruikt op onze iPhones. Daarmee worden we nog zekerder van het feit dat wij degenen zijn die op onze iPhone inloggen. Het is dus een goede toepassing. Het voorbeeld van hier beneden in het gebouw vind ik nog mooier. Daar heb ik destijds wel mijn vraagtekens bij geplaatst, want dat was een besluit van de Tweede Kamer om ons specifiek beter te kunnen beschermen. Het zijn dus twee specifieke toepassingen. Maar de vraag is of de afweging gemaakt kan worden van de voor- en de nadelen van deze specifieke technologie met betrekking tot het gevaar dat je mensen onterecht herkent. Dat hoop ik in de brief terug te zien. Dat is mijn vraag aan de Minister. Ik zal het bij één vraag houden, maar daardoor is deze wel iets langer dan wanneer dit in tweeën zou zijn gegaan, voorzitter. Maar mijn grootste zorg is dat gezichten worden herkend terwijl het gewoon een fout blijkt te zijn. Het gaat mij om de fouten in het systeem. Die vormen hier volgens mij het grootste risico.

Minister **Grapperhaus**:
Ik was van zins om dat soort elementen in de brief mee te nemen.

De **voorzitter**:
Prima. Dan gaan we verder. Ik wijs er nogmaals op dat we om 14.30 uur stemmingen hebben en dat daarna nog de regeling komt. We zijn dus zomaar tot 15.00 uur bezig. We hebben maar tot 15.30 uur en we moeten ook nog een tweede termijn doen. Dus ik ga u niet langer ophouden.

Minister **Grapperhaus**:
Als ik de bankrekening van mevrouw Buitenweg heb gehad, dan zijn we volgens mij een enorm eind verder. Voor het specifieke voorbeeld van de bankrekening geldt dat storing doorgaans betekent dat klanten tijdelijk niet bij de bankrekening kunnen. Het betekent niet dat gegevens weg zijn. De storing is meestal bij ongeveer de helft van de banken. Niettemin is het belangrijk om de digitale weerbaarheid structureel te verhogen, zodat de continuïteit en veiligheid zijn geborgd, ook waar geen analoge terugval-opties zijn. Dat betekent dat je er hier voor moet zorgen dat de bank en de burger er allebei van doordrongen zijn dat dit kan gebeuren en dat ze een back-up moeten hebben. En die back-up moet dan niet afhankelijk zijn van het systeem dat mogelijk onder vuur komt te liggen.

Mevrouw **Buitenweg** (GroenLinks):
Ik vraag me toch af wat u aan burgers vraagt. Moeten we elke week voor de zekerheid de gegevens van onze bankrekeningen printen? Ik citeer uit het Cybersecuritybeeld Nederland 2019. Op de vraag of er back-ups zijn van onze saldi en of die back-ups niet kunnen worden gemanipuleerd – want het gaat dan over manipulatie – zegt de NCTV: «Het antwoord

hierop is lastig te geven.» Het is voor ons allemaal wel fijn om te weten of, als er sprake is van manipulatie, de back-ups dan ook gemanipuleerd kunnen zijn. En wat moeten wij doen om dat te voorkomen? Moeten wij wekelijks een printje maken van onze rekeningen? Of is daar toch nog iets anders voor?

Minister **Grapperhaus**:
Laat me even dit zeggen: primair moet de sector – de bankensector in dit geval en de financiële sector – hier weerbaar op zijn. De financiële sector is een van de sectoren geweest die hier de afgelopen jaren het meest mee aan de gang is gegaan. Dat is proefondervindelijk bewezen. Die sector is het meest voorop gaan lopen. De weerbaarheid moet primair daar zitten. Maar ik benadruk ook dat je je moet realiseren, ook als burger, dat je geen analoge terugvaloptie hebt. Je zou er inderdaad niet onverstandig aan doen om je goed op te hoogte te stellen van hoe dit zich ontwikkelt bij je eigen bankrekening. Of je daarbij elke week je afschriften uitprint, is vers twee. Maar er zijn ook mensen die ongeveer eens per twee maanden op hun bankrekening kijken. Tegen hen zeg ik echt dat ze zich moeten realiseren dat het belangrijk is om zelf goed op de hoogte te zijn.

De **voorzitter**:
Dank u wel. Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Mevrouw Buitenweg vroeg: heeft Nederland genoeg technische knowhow om cyberaanvallen te kunnen attribueren? Dat is een belangrijke vraag. Digitale veiligheid is een grensoverschrijdend vraagstuk. Digitale aanvallen kunnen vaak nagenoeg anoniem worden uitgevoerd. Dat bemoeilijkt de attributie en de opsporing van de daders aanzienlijk. Maar toch beschikken de operationele diensten over genoeg middelen en expertise om het technisch attribueren van aanvallen zo veel mogelijk te kunnen doen. Daar is inderdaad de juiste technische knowhow voor nodig. Daarom staat ook in de NCSA, de Nederlandse Cybersecurity Agenda, dat de operationele slagkracht van de diensten moet worden versterkt. U heeft vorig jaar gezien dat we daar extra middelen voor ter beschikking hebben gesteld, boven op de extra middelen in het regeerakkoord. Daar zullen we inderdaad echt weerbaar in moeten zijn.
Voorzitter. Ik doe een aantal vragen enigszins door elkaar heen. De eerste, van de heer Verhoeven, gaat nog over cyberattributie. Het kabinet heeft niet het voornemen om zich in te zetten voor de oprichting van een internationaal instituut voor de attributie van cyberaanvallen. Het bestaande internationale recht is in beginsel gewoon van toepassing op cyberspace. Dit kabinet denkt dat het nu niet wenselijk is om te gaan pleiten voor een nieuw internationaal gremium. Dan krijgen we hele lange verdragsonderhandelingen, terwijl Nederland van mening is dat er al bestaand recht is dat dit zou moeten dekken. Wel is het heel erg van belang om de internationale rechtsorde op dit punt verder te ontwikkelen. Dat betekent dus ook dat we gezamenlijk moeten optreden, in respons, bij cyberoperaties.
Ik meen dat hier door mevrouw Laan en door mevrouw Buitenweg ook nog vragen over werden gesteld. Dan gaat het om het EU Cybersanctieregime en de EU Cyber Diplomacy Toolbox. Dat zijn daar goede voorbeelden van. Overigens zal mijn collega van BZ op korte termijn een brief aan uw Kamer sturen naar aanleiding van onder meer de motie van de heer Verhoeven en mevrouw Bruins Slot, waarin wordt verzocht om een weergave van de initiatieven ten behoeve van het bestendigen van de internationale rechtsorde in het digitale domein.
De heer Verhoeven vroeg ook naar de ethische hackers. Er is een Coordinated Vulnerability Disclosure-programma van de rijksoverheid. Daar werkt het NCC, het Nationaal Centrum Cybersecurity, nauw mee

samen. Of nee, het is natuurlijk het Nationaal Cyber Security Centrum, het NCSC. Ethische hackers kunnen zich daar melden. Ik heb al vaker gezegd dat ik daar echt waarde aan hecht. We zetten ons in om dit op Europees niveau zo veel mogelijk verder te versterken.
Mevrouw Laan vroeg: op welke wijze stimuleren we nou dat we ook Europese en/of Nederlandse aanbieders hebben? Hoe doen we dat in aanbestedingstrajecten? De nationale veiligheidsrisico's die door die afhankelijkheden kunnen ontstaan, brengen we steeds verder in kaart als kabinet. We bekijken hoe we die inderdaad door inkoop en aanbesteding meer kunnen beheersen. U heeft dat ook gezien in mijn brief over de statelijke actoren van twee maanden geleden. Daarin hebben we ook een hoofdstukje gewijd aan de investeringstoets. In 2018 is door Binnenlandse Zaken en de NCTV voor veilige inkoop en aanbesteding een instrumentarium ontwikkeld. Dat is al ingevoerd door het kabinet. Zoals gezegd maken we dat nu ook geschikt voor onderdelen van de vitale infrastructuur. We werken ook in het kader van inkoop en aanbesteding in de Nederlandse Cybersecurity Agenda aan aanvullende cybersecuritycriteria bij de inkoop van eigen ICT-middelen door de overheid.
Naar aanleiding van de door de Algemene Rekenkamer gesignaleerde problematiek bij Rijkswaterstaat vroeg mevrouw Buitenweg of de collega's dat onderwerp voldoende prioriteit geven. Ik weet dat mijn collega met u in debat is gegaan over het rapport van de Rekenkamer en de aanbevelingen daaruit. Die Minister heeft aangegeven alle aanbevelingen over te nemen. Laat duidelijk zijn dat het rapport ook mijn volle aandacht heeft. In de brief die ik u heb gestuurd bij de aanbieding van het Cybersecuritybeeld Nederland heeft u gezien dat er een hele passage is waarin ik heb aangegeven dat ik meer ga sturen op toezicht op de daadwerkelijke uitvoering. Ik ga alle noodzakelijke cybersecuritymaatregelen ook bijhouden, want dat is ook heel belangrijk. Je kunt wel dijken aanleggen, maar je moet ze vervolgens permanent bewaken. Deze zomer zal ik met de NCTV gaan zitten om dit ook verdere vormgeving te bieden.
De heer Van Dam vroeg in het verlengde hiervan – ik zie het althans in het verlengde hiervan – wat we eigenlijk voor de gewone burger doen in het geval van cybercrime, naast het Nationaal Cyber Security Centrum en het Digital Trust Center. Laat ik vooropstellen dat ik het er volledig mee eens ben dat er meer aandacht voor de burger moet zijn. Dat zeg ik niet gratuit, zo van «de burger is er ook». De weerbaarheid van burgers en bedrijven moet nog steeds omhoog. Het Cybersecuritybeeld waarschuwt daar ook voor. Ik vind dat daar echt nog stappen in moeten worden gezet.
We zijn het afgelopen jaar al stevig aan de slag gegaan ten aanzien van de burger. Er is geïnvesteerd in een preventiecampagne. Het eerste voorbeeld daarvan is de campagne Eerst checken, dan klikken! Die is echt gericht op de burger. Na de zomer gaat die zich vooral richten op de veiligheid van hard- en software. Er zijn een paar websites, onder andere veiliginternetten.nl, waarop de juiste informatie te vinden is die de burger verder moet helpen. Ook Slachtofferhulp Nederland heeft een nieuw onlineplatform gelanceerd met onder andere specifieke informatie om die groep slachtoffers te helpen.
In een ander verband heb ik aan uw Kamer gemeld dat we ook samenwerkingsverbanden hebben met instanties zoals Marktplaats, om ervoor te zorgen dat burgers eerder geholpen worden ten aanzien van wat hen aan cybercrime overkomt en dat burgers digitale hulpmiddelen krijgen aangeboden. Verder werken we nog steeds aan het verhogen van de kennis op het gebied van cybercrime. Dat is natuurlijk het allerbelangrijkste als het gaat om de burger. Het Belgische team is een heel klein team. Het zijn 30 personen. Zij doen eigenlijk voor een belangrijk deel wat bij ons het NCSC al doet. Ik durf echt te beweren dat we hier als overheid al heel veel stappen zetten en blijven zetten om de burger een heel stuk verder te helpen. Maar het heeft de continue aandacht, al was het maar omdat de weerbaarheid van de burger op het gebied van cybersecurity

van heel groot belang is. We kunnen onze digitale dijken nog zo stevig maken, maar dan helpt dat nog niet goed.
Voorzitter. Ik heb nog een vraag van mevrouw Laan. Zij vroeg of we iets kunnen doen met iemand die door vijf landen reist. Ik kan het niet nalaten om met enige verheugenis te zeggen dat mijn wetgeving op het gebied van uitwisseling van passagiersinformatie nu door beide Kamers is aangenomen en eergisteren is ingevoerd. Ik geef toe: het is een beetje een reclamepraatje, maar dat helpt ook op dit onderwerp. Daarnaast zal ik, als u dat goedvindt, bij u in een brief terugkomen op hoe we die technologische systemen op een goede manier optimaal kunnen inzetten om het soort reizen dat mevrouw Laan beschreef in de toekomst te voorkomen.

De **voorzitter**:
Ik hoor een bel. Dit zal ongetwijfeld de stemmingsbel zijn. We gaan om 14.30 uur stemmen. Ik ga de vergadering dus nu schorsen.

Minister **Grapperhaus**:
Ik ben er bijna doorheen.

De **voorzitter**:
Ja, maar dat gaan we niet meer redden. Ik stel voor dat we doorgaan zodra we hier weer terug zijn. Dat is – als u tenminste nergens anders hoeft te zijn – na de vraag van de heer Van Dam. Ik hoop dat u in de gaten kunt houden wanneer dat is. Dan treffen we elkaar hier weer.
Ik schors de vergadering voor onbepaalde tijd.

De vergadering wordt van 14.27 uur tot 15.23 uur geschorst.

De **voorzitter**:
We gaan snel beginnen. Wij waren toe aan de laatste antwoorden van de Minister in zijn eerste termijn.

Minister **Grapperhaus**:
Voorzitter. Ik zal er heel snel doorheengaan.
Mevrouw Laan vroeg nog naar cybersecurityonderzoek. Daar zetten we stevig op in. Het verkenningstraject wordt afgerond en daarop vooruitlopend zijn er al financiële investeringen gedaan. Dit najaar wordt in het kader van de Nationale Wetenschapsagenda nog eens 5,15 miljoen euro beschikbaar gesteld. U wordt over de voortgang binnenkort geïnformeerd door mijn collega, de Staatssecretaris van EZK.
Nog even over het Berlijnse verhaal en het gebruik van big data. Op de buitengrens vinden natuurlijk controles plaats op basis van de Schengengrenscode, waarbij de datasystemen SIS en SLTD systematisch worden bevraagd. Dat zijn de big-datasystemen waar het over gaat. Dit staat natuurlijk naast de mogelijkheid om niet-systematische politiecontroles uit te voeren binnen grenzen, zoals dat in Nederland gebeurt met het Mobiel Toezicht Veiligheid.
Dan had ik nog een vraag van de heer Verhoeven over het scannen van kwetsbaarheden. Uit het CSBN 2019 komt een zorgwekkend beeld van de digitale dreiging naar voren. In 2018 heeft het kabinet de Nederlandse Cybersecurity Agenda gepresenteerd. Inmiddels zijn we druk aan de gang met de uitrol daarvan. Het laatste Cybersecuritybeeld laat wel zien dat we de ingeslagen weg moeten voortzetten. Dat heeft u ook eerder van mij gehoord in deze eerste termijn. Versterkte inzet op digitale weerbaarheid is heel erg nodig en daarom gaan we de komende tijd onder mijn regie werken aan een systeem van structurele, adaptieve risicobeheersing en toezicht. We zetten in op een aantal maatregelen, maar die zijn allemaal beschreven in het Cybersecuritybeeld, dus de uitwerking daarvan zal ik u op dit moment besparen.

Voorzitter. Er is geen vraag over gesteld, maar ik wil nog opmerken dat ik dinsdag bij uw Kamer, conform afspraak, de antwoorden op de vragen inzake de evaluatie van de Wet veiligheidsregio's heb ingeleverd. Ik ga ervan uit dat met die beantwoording en de bespreking met uw commissie de evaluatieopdracht is afgerond. Die wordt dan nu opgenomen in de instellingregeling en vervolgens besproken in de ministerraad.
Dat was mijn eerste termijn, voorzitter.

De **voorzitter**:
Hartelijk dank. Ik kijk even of er nog behoefte is aan een tweede termijn. Die is er. Heel kort dan. Ik geef als eerste het woord aan mevrouw Buitenweg. De Minister moet om 15.30 uur weg, dus we gaan het echt heel kort houden.

Mevrouw **Buitenweg** (GroenLinks):
De Minister moet om 15.30 uur weg. Dan is mijn tweede termijn dat ik zeg dat ik graag een VAO wil aanvragen. Ik dank de Minister voor zijn uitleg, ook in de brief, over C2000. Het is een voorbeeld van iets waarover we anders zijn gaan denken en waarop nu ook anders gehandeld wordt. Dat is van belang.
De brief over de gezichtsherkenning gaat tot mij komen. Ik blijf daarbij nog met één punt zitten. We doen een investeringstoets, maar hoe gaan we om met allerlei bedrijven die ondertussen voet aan de grond krijgen in Nederland? Dat blijft een punt van zorg en dat zal ik in het VAO nog verder adresseren.

De **voorzitter**:
Dank u wel. Mevrouw Laan?

Mevrouw **Laan-Geselschap** (VVD):
Helaas, het is 15.30 uur. En 15.30 uur is 15.30 uur toch?

De **voorzitter**:
Als u nog snel een vraag stelt, kunt u misschien nog een antwoord krijgen.

Mevrouw **Laan-Geselschap** (VVD):
Mijn vraag is in hoeverre de Minister bereid is om na te denken over de financiële consequenties van het kiezen voor veiligere systemen dan waar nu voor gekozen wordt.

De **voorzitter**:
Dank u wel. Meneer Verhoeven?

De heer **Verhoeven** (D66):
Dank. Ik zou het fijn vinden om over de brief die in oktober komt een keer goed met elkaar door te praten, maar dat moeten we zelf regelen, via de procedurevergadering. Verder hoor ik algemene termen over adaptieve controle, maar ik wil graag wat meer concrete dingen horen over de scan van de vitale infrastructuur. Anders zal ik daar bij het VAO nog op terugkomen.
Ik heb nog één andere vraag, over de verkenner voor het cybersecurity-instituut. Er is ooit in de Kamer een motie ingediend door VVD en D66. Daarin werd gevraagd om een cybersecurityinstituut op te zetten en daar kwam een verkenner voor. Daar hoor ik weinig meer van.
Dat was het, voorzitter.

De **voorzitter**:
Dank u wel. Meneer Van Dam? Nee? Dan de Minister voor zijn tweede termijn.

Minister **Grapperhaus**:
Voorzitter. Ik begin even met het punt van de verkenner. Daar zal ik snel in een briefje naar u op terugkomen. Ik moet bekennen dat ik op dit moment die kennis niet paraat heb. Dat is één.
Ik zal ook nog even proberen om een aantal dingen over de kwetsbaarheid van die scan op een rij te zetten, maar dat zal volgende week worden. Ik heb een aantal dingen hier niet genoemd, omdat die terugkomen in het Cybersecuritybeeld Nederland en ik dacht dat dat dan een herhaling zou zijn. Maar ik zal het nog even in een brief zetten en als u dat onvoldoende uitgewerkt vindt, dan hoor ik dat op het VAO.
Mevrouw Laan vroeg naar de afweging op het punt van veiligheid en kosten. Niet alleen in de C2000-brief, maar ook in de brief over de statelijke actoren staan natuurlijk al een aantal overwegingen. Ik kan niet garanderen dat ik het voor het VAO in orde heb, maar ik wil wel toezeggen dat ik nog eens in een brief op een rij zet hoe we daar precies mee omgaan. Dan kom ik daar na de zomer bij u op terug.
Ik pel het laatste deel van de papieren nu af en kom op de vraag van mevrouw Buitenweg, die weliswaar geen vraag had, maar een VAO aanvroeg, net als enkele andere leden. Ik hoop dat dit VAO nog voor de zomer kan, dus ergens in de komende twee weken. Dat zou wel moeten. Ik weet natuurlijk niet waar u het over wilt hebben en dat is ook niet aan mij, maar er zijn een paar onderwerpen waar ik verder mee moet.

De **voorzitter**:
Goed. Dat is overigens ook de wens van enkele leden.
Ik constateer dat er een VAO is aangevraagd met als eerste spreker mevrouw Buitenweg. Er is een uitdrukkelijk verzoek aan de plenaire Griffie om dit voor het zomerreces in te plannen.
Ik neem nog even de toezeggingen door.
– De Minister zal de Kamer na het zomerreces 2019 informeren over de opvolging van het C2000-systeem, in lijn met het advies van de AIVD.
– De Minister zal de Kamer in september een brief sturen over de uitfasering van het Waarschuwings- en alarmeringssysteem en de daarmee gepaard gaande invoering van NL-Alert. Hij zal daarbij specifiek ingaan op de vraag of beide systemen naast elkaar kunnen bestaan.
– De Minister zal de Kamer, mede namens de Minister voor Rechtsbescherming, in de eerste helft van het vierde kwartaal van 2019 een brief sturen over het gebruik van technologieën als gezichtsherkenningssoftware voor de opsporing en de daarmee gepaard gaande risico's.

Ten slotte:
– De Minister zal de Kamer een brief sturen over de toepassing van technologieën rond het uitwisselen van passagiersgegevens in het kader van de opsporing.

Daar is nog geen termijn aan gegeven. September, hoor ik. Oké, die brief komt in september 2019.

Mevrouw **Laan-Geselschap** (VVD):
In de laatste zin van de Minister deed hij nog een toezegging voor een brief. Die is nog niet genoemd.

De **voorzitter**:
Nog een brief?

Minister **Grapperhaus**:
Ja. De brief over de verkenner komt voor het VAO, dus dat is ergens de komende week, want het VAO zal ergens in de komende week of de week erna moeten plaatsvinden.

De brief die ik aan mevrouw Laan heb toegezegd komt na de zomer. En met na de zomer bedoel ik ergens heel snel in september of begin oktober.

De **voorzitter**:
En we hebben allemaal scherp waar die brief over ging?

Minister **Grapperhaus**:
Die brief ging over de vraag hoe je je afweging maakt als iets meer kost maar ook meer veiligheid biedt.

De **voorzitter**:
Meneer Verhoeven nog?

De heer **Verhoeven** (D66):
De Minister suggereerde dat hij nog wat nadere info zou opschrijven over de kwetsbaarheid van de scan.

Minister **Grapperhaus**:
Die brief komt ook voor het VAO. Ik lees net dat de Staatssecretaris van EZ binnenkort al met die brief over dat cybersecurityinstituut komt. Het zou kunnen dat de verkenner daar ook in voorkomt.

De **voorzitter**:
Nou, u bent weer op uw wenken bediend.

De heer **Verhoeven** (D66):
Maar die scan is een ander punt, hè.

Minister **Grapperhaus**:
Dat weet ik. Het gaat niet over een verscanner of zo.

De **voorzitter**:
Oké. Ik ga de vergadering sluiten. Ik dank de Minister, zijn ambtenaren, de leden, de ondersteuning en de mensen op de publieke tribune en elders en ik wens u allen nog een mooie dag toe. Ik sluit de vergadering.

Sluiting 15.32 uur.