Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 **Informatie- en communicatietechnologie (ICT)**

30 821 **Nationale Veiligheid**

Nr. 650

VERSLAG VAN EEN ALGEMEEN OVERLEG
Vastgesteld 21 november 2019

De vaste commissie voor Justitie en Veiligheid heeft op 30 oktober 2019 overleg gevoerd met de heer Grapperhaus, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 25 juni 2019 inzake reactie op vragen gesteld tijdens het algemeen overleg Nationale Veiligheid van 20 juni 2019 over de wenselijkheid van een scan van kwetsbaarheden in de context van cybersecurity en het belang van publiek-private samenwerking daarbij (Kamerstukken 30 821 en 26 643, nr. 86);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 16 juli 2019 inzake reactie op verzoek commissie over de rol van de overheid en IT-branche in cybersecurity (2019D31225);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 6 augustus 2019 inzake onderzoeksrapport WODC kwetsbaarheden industriële controlesystemen (Kamerstukken 26 643 en 30 821, nr. 625);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 29 oktober 2019 inzake voortgang versterkte aanpak cybersecurity (Kamerstuk 26 643, nr. 647).**

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

De voorzitter van de commissie,
Van Meenen

De griffier van de commissie,
Hessing-Puts

kst-26643-650
ISSN 0921 - 7371
's-Gravenhage 2019

Voorzitter: Van Meenen
Griffier: Burger

Aanwezig zijn vijf leden der Kamer, te weten: Van den Berge, Van Dam, Van Meenen, Middendorp en Verhoeven,

en de heer Grapperhaus, Minister van Justitie en Veiligheid.

Aanvang 15.05 uur.

De **voorzitter**:
Welkom bij het algemeen overleg Cybersecurity van de vaste commissie voor Justitie en Veiligheid. Ik heet de leden hartelijk welkom en ook meneer Koopmans, want die is formeel geen lid van deze commissie.

De heer **Middendorp** (VVD):
Middendorp, voorzitter.

De **voorzitter**:
Neem me niet kwalijk; jullie lijken een beetje op elkaar. Meneer Middendorp. Ik vraag de leden of zij er bezwaar tegen hebben dat de heer Middendorp namens de VVD het woord voert. Ja, meneer Verhoeven?

De heer **Verhoeven** (D66):
Als het nou de heer Koopmans betrof, dan zou ik getwijfeld hebben, maar nu het de heer Middendorp betreft, kan ik niet anders dan enthousiast zijn.

De **voorzitter**:
Sorry, sorry, sorry. Dan gaan we dat doen. Ik heet de Ministers en ambtenaren van harte welkom, evenals de mensen op de publieke tribune, onze ondersteuning en natuurlijk de leden. We hebben tot 18.00 uur. Zelf zal ik u om 17.00 uur moeten verlaten, maar met dit aantal leden lukt het wellicht om al om 17.00 uur klaar te zijn. Ik zou willen voorstellen om spreektijden te hanteren van vier minuten. Als u daarmee akkoord bent, zou ik als eerste het woord willen geven aan de heer Van Dam van het CDA.

De heer **Van Dam** (CDA):
Voorzitter, is het toegestaan om hier te blijven zitten of moet ik gaan staan?

De **voorzitter**:
U mag blijven zitten.

De heer **Van Dam** (CDA):
Ik mag blijven zitten. Dat geldt eigenlijk alleen voor de mensen die als eerste het woord voeren. De anderen worden geacht te gaan staan, heb ik begrepen.
Voorzitter. Ik wil beginnen met een woord van dank aan de Minister. We hebben het Cybersecuritybeeld Nederland al eerder besproken in een AO Nationale veiligheid, volgens mij op verzoek van de heer Verhoeven. Misschien was dat een beetje oneigenlijk, maar het is wel goed dat we dat toen al meteen gedaan hebben. Het is ook goed dat de Minister als coördinerend Minister rapporteert over de cyberveiligheid. Er was destijds bij de begeleidingsbrief bij dat CSBN volgens mij ook meteen een soort eerste voortgangsrapportage over hoe het nu gaat met de plannen. Ik wil niet meteen negatief zijn over die brief, maar het was natuurlijk nog informatie op een wat abstract niveau, op een hoofdlijnenniveau. Vandaar mijn eerste vraag aan de Minister: hoe gaat de Minister zeker in de komende tijd tot een wat tastbaardere verantwoording komen, zodat we

als Kamer iets concreter kunnen volgen hoe die ontwikkelingen zijn? We hebben een mooi blad gekregen met verschillende domeinen; ik laat het, ook voor de kijkers thuis, even zien. Het zou ongelofelijk fijn zijn als we bijvoorbeeld ook op zo'n manier op die verschillende terreinen wat meer over de voortgang te horen krijgen.
Voorzitter. Dan de VPN-Pulsecase en alles wat daaruit wegkomt, ook de plannen die de Minister heeft aangekondigd en die we ook besproken hebben in een mondeling vragenuur om – in mijn termen – wat meer druk te zetten op mensen of bedrijven die geen adequate maatregelen nemen om hun beveiliging op orde te hebben. Ik moet zeggen dat dat leuk klinkt. We zijn ook allemaal naar de microfoon gehold om onze verbazing en afschuw uit te spreken, maar ik denk dat het nog belangrijker is om te kijken hoe het nou gaat met dat hele toezichtsysteem en ook met de eigen verantwoordelijkheid van de bedrijven in die vitale sector. Over het algemeen denk ik dat die bedrijven ook zelf niets liever zouden willen dan op dat terrein gewoon de goede dingen doen. In dat kader heb ik een aantal vragen aan de Minister, ook over de implementatie van de Wet beveiliging netwerk- en informatiesystemen. Dat is overigens een vreselijke naam. Waarom hebben ze dat niet gewoon de Wet cybersecurity genoemd? Maar dat terzijde.
Mijn vraag is hoe het nou zit. Hoe zit het nou met die toezichthouders? De Minister schrijft dat het Nationaal Cyber Security Center niet een rol moet hebben in het aanspreken van bedrijven; dat moeten de toezichthouders gaan doen. Maar zijn die toezichthouders daarop voorbereid? Hebben zij voldoende kennis? Wat is het kennisniveau van de toezichthouders bij het vervullen van die rol? En hoe zit het met de kennis van het NCSC zelf op dit vlak? Een heleboel van die vitale bedrijven hebben heel veel te maken met procestechnologie en met de ICT op dat vlak. Dat schijnt bijzondere kennis te zijn. Is die voorhanden binnen het NCSC en ook bij die toezichthouders? Zijn zij op dat punt voldoende voorbereid?
De Minister kondigt aan dat er een vertrouwelijk inspectiebeeld zal komen van de Inspectie JenV om te kijken hoe de toezichthouders hun rol vervullen. Is er een mogelijkheid om dat vertrouwelijke inspectiebeeld ook te delen met de Kamer, desnoods vertrouwelijk, zodat ook wij onze rol daarin kunnen blijven vervullen?
Een laatste vraag op dit vlak: hoe zit het met de wederkerigheid van de informatie? Er is bij het NCSC veel informatie over dreigingen die plaatsvinden en er is ook overleg met de diensten, maar hoe komt die informatie ook weer terug bij bedrijven in die vitale sector, met name ook binnen sectoren? Ik noem maar wat: als je in de watersector dingen zit te doen, of dat nou om drinkwater gaat of om waterkeringen, kan ik me voorstellen dat er informatie is die specifiek daarop betrekking heeft. Hoe kunnen we dat organiseren?
Voorzitter, u gaat toch niet zeggen dat ik al door mijn tijd heen ben?

De **voorzitter**:
Jawel.

De heer **Van Dam** (CDA):
Dan rond ik af. Zullen we het zo doen?

De **voorzitter**:
Ja.

De heer **Van Dam** (CDA):
Tot slot, voorzitter. Ik maak mij wat zorgen... Laat ik het positief formuleren: op het vitale gebied gebeurt er op het punt van cybersecurity heel veel, maar hoe zit het nou met de bedrijven daaronder en hoe zit het met de burger? Om een voorbeeld te noemen: ik ben erachter gekomen dat het DTC, het Digital Trust Center, niet een instituut is dat langer gaat

bestaan, maar dat dat een project of programma is dat zal lopen tot eind 2020. Het wordt geëvalueerd, maar wat gaat daar gebeuren? Wat is de ambitie? De Minister kan zeggen dat hij daar niet van is en dat ik bij EZK moet zijn, maar dan spreek ik hem toch aan in zijn coördinerende rol om te zeggen hoe dit moet. En hoe zit het met de burger? Mijn ervaring is dat je zonder breedtesport ook geen topsport kunt bedrijven. Ik maak mij dus zorgen over wat nu het perspectief is van de burger en wat de handelingsmogelijkheden voor de burger zijn om met de cyberveiligheid aan de slag te gaan. Graag een reactie.
Dank u wel.

De **voorzitter**:
Dank u wel. Dan geef ik graag het woord aan de heer Verhoeven van D66.

De heer **Verhoeven** (D66):
Dank u wel, voorzitter. Er zijn allerlei belangrijke adviseurs en instituten die in de afgelopen jaren iets hebben gezegd over onze digitale veiligheid. De Wetenschappelijke Raad voor het Regeringsbeleid en de NCTV wijzen op digitale ontwrichting. De AIVD spreekt over de afhankelijkheid van en dreiging vanuit Rusland en China. De Rekenkamer zegt dat onze vitale waterwerken niet goed beschermd zijn. Het Rathenau Instituut zegt dat overheden en bedrijven onvoldoende beschermd zijn tegen cyberdreiging. Er zijn ook allerlei organisaties die bellen, sommige sturen een brief, en die pleiten voor een digitaal deltaplan. Er zijn heel veel verschillende, serieuze, breed gedeelde geluiden over dit onderwerp.
Ik las vorige week tijdens het reces – zoals u weet is reces geen vakantie – het boek van Huib Modderkolk. Daarin staat ineens een bedrag van 340 miljoen. Uit een gesprek met de veiligheidschefs en de premier bleek dat dit nodig zou zijn voor een minimale investering in cybersecurity. Dat zou het absolute minimum zijn om Nederland digitaal veilig te maken. Ze hebben natuurlijk het deksel op de neus gekregen. Althans, voor een groot deel. Er is wel geïnvesteerd in cybersecurity, maar niet 340 miljoen. Het bedrag dat daar wordt opgevoerd, is mij onbekend en de onderbouwing ook. Ik zou het heel goed vinden als we toch ook met elkaar via dit AO onderzoeken wat nou de behoefte is aan investeringen bij Defensie, de diensten, het Nationaal Cyber Security Centrum, de vitale infrastructuur, op het gebied van die digitale veiligheid. Dus mijn vraag aan de Minister is: is hij bereid om onderzoek te laten doen naar de behoefte aan overheidsinvesteringen voor cybersecurity? Dat was mijn eerste punt.
Het gaat overigens niet alleen om geld. Het gaat ook om – mijn gewaardeerde collega van het CDA gebruikte het woord net ook al – een goede coördinatie, een goede afstemming en een goede samenwerking. Er zijn ongelooflijk veel organisaties mee bezig. Nederland is hier ook goed in, maar het kan ook nog wel beter. Ik noem als voorbeeld het Pulse Secure VPN-verbindingsprobleem dat er laatst was. Daar heeft het NCSC een melding voor uitgedaan, maar bedrijven hebben dat niet, of in ieder geval niet allemaal, goed en actief opgepakt. We hebben laatst in de Tweede Kamer bij het mondeling vragenuur ook gesproken over doorzettingsmacht. Toen sprak de Minister zelfs even over een autoriteit. Ik ben gek op autoriteiten en ik vind doorzettingsmacht ook heel belangrijk, maar toen heb ik ook aan de Minister gevraagd: moet dit dan een nieuwe autoriteit zijn of is dit vooral de bestaande rol van het Nationaal Cyber Security Centrum die versterkt moet worden? Hoe gaan we die rol van die organisatie verbeteren te midden van al die andere partijen die ook actief zijn, zoals de diensten, de NCTV en verschillende ministeries? Dat zou mijn tweede blokje zijn.
Onder de nieuwe Wet beveiliging netwerk- en informatiesystemen, die net ook al werd genoemd, krijgen de zogeheten essentiële diensten ook een zorgplicht om hun cybersecurity op orde te hebben. Als er nou zo'n

zorgplicht zou zijn of komen, zou het patchen van bijvoorbeeld zo'n Pulse Secure-kwetsbaarheid dan onder die zorgplicht zijn gevallen? En zou er dan dus ook een boete zijn opgelegd door de toezichthouder, in dit geval het Agentschap Telecom?

De heer **Van Dam** (CDA):
Ik wil even checken of de heer Verhoeven nog lid is van D66, wat volgens mij een liberale partij is. Ik denk dat bij dat liberale toch ook hoort dat de samenleving veel zelfverantwoordelijkheid pakt. Is nou echt zijn beeld van de bedrijven in de vitale sector – laten we het daar even toe beperken – dat die allemaal achter de broek moeten worden gezeten door autoriteiten? Ik heb begrepen dat er nu een patchorder aankomt. Hoe zit dat? Hoe kijkt hij aan tegen de verdeling van verantwoordelijkheden en ook de eigen verantwoordelijkheid in die sector?

De heer **Verhoeven** (D66):
Mijn lidmaatschap van D66 is onomstotelijk; dank daarvoor. De partij is sociaal-liberaal. Dat betekent dat we dus niet alleen maar denken in termen van verantwoordelijkheid bij bedrijven, maar ook aan het beschermen van de samenleving als geheel. Bij cybersecurity is dat wel heel belangrijk. Collega Van Dam wijst op twee dingen. Hij verwijst naar de woorden van de Minister van Justitie en Veiligheid over een autoriteit. Die heeft gezegd: er is toch een bepaalde autoriteit nodig in de coördinatie. Dat heeft de heer Van Dam zojuist zelf ook gezegd. Ik denk alleen dat die autoriteit er al is, namelijk het NCSC, maar dat haar rol nog wat moet worden versterkt.
Het andere is de Wet beveiliging netwerk- en informatiesystemen, die er ook aankomt. Daar staat die zorgplicht in. Mijn vraag was een beetje: hoever reikt zo'n zorgplicht nou? Want je hoort het woord «zorgplicht» vaak. Ik heb een concreet voorbeeld genoemd om te kijken of dat onder die zorgplicht viel. Dat was het voorbeeld dat de heer Van Dam net zelf ook noemde: de Pulse Secure-kwetsbaarheid. Als er zoiets is en veel bedrijven worden daardoor geraakt, dan zou ik wel willen weten of er een zorgplicht is. Dan betekent dit dat bedrijven ook zelf de verantwoordelijkheid hebben om dat op te lossen.

De heer **Van Dam** (CDA):
Ik denk dat we een beetje moeten uitkijken dat als we een heel systeem aan het opbouwen zijn – dat is toch waar die Wbni voor staat – en er zich in de tussentijd een incident voordoet, we niet meteen allerlei maatregelen treffen die een beetje haaks staan op wat die wet met zich meebrengt. Die wet brengt met zich mee – daar hebben we het in de Kamer uitgebreid over gehad – dat er toch ook een heel grote verantwoordelijkheid bij bedrijven zelf ligt. Ik ben het er helemaal mee eens dat als er bedrijven zijn die coûte que coûte niet willen, je daar dan zeker iets mee zult moeten. Daar wordt ook in voorzien door de inspecties. Daar ben ik een beetje kwijt wat D66 nu wil. Het klinkt mij te sociaal en te weinig liberaal in de oren. Dat is misschien een klein advies.

De heer **Verhoeven** (D66):
Dank u wel. Ik ben niet verder gegaan dan hetgeen al in een wet wordt voorgesteld om te kijken wat de reikwijdte daarvan is in het belang van de veiligheid van ons land.

De **voorzitter**:
Gaat u verder. U heeft nog een minuut.

De heer **Verhoeven** (D66):
We, collega's samen met de VVD, hebben in de Kamer vaak een punt gemaakt van het scannen naar kwetsbaarheden, om het scannen van de

vitale infrastructuur van alle overheidssystemen in Nederland nou eens serieus aan te pakken. Daar wordt ook door veel verschillende organisaties voor gepleit. De motie is aangenomen. Het was een groot succes. Kan de Minister nu eens schetsen hoe de motie wordt uitgevoerd? Hoe wordt het proces van scannen ingericht? Wat gaat er precies gebeuren om dat scannen van die vitale infrastructuur in Nederland op een goede manier te doen?
Dan nog even het WRR-rapport over de digitale ontwrichting. De aanbevelingen zijn onder andere: het opstellen van een cyberafhankelijkheidsbeeld en het delen van kennis en paraatheid. Voor paraatheid werd zelfs de metafoor van een digitale brandweer gebruikt. Daar werd verschillend op gereageerd door de betrokken organisaties. Wat is nu met betrekking tot die paraatheid de stap die de Minister wil gaan zetten? In dat kader vond in 2017 de publiek-private cybersecurityoefening ISIDOOR II plaats. Hoe en wanneer wordt hier opvolging aan gegeven? Want ik hoor ook van veel betrokken organisaties en deskundigen dat oefenen belangrijk is.
Voorzitter. Dan mijn allerlaatste punt: 112. Het zal hier misschien niet thuishoren, maar als we het over cybersecurity hebben, dan vind ik dat dit toch ook iets is dat hier wel genoemd moet worden. We hebben het in het mondeling vragenuur – ik denk dat het afgelopen zomer vlak na het reces is geweest – gehad over een back-upsysteem. Een tweede aanbieder kan ervoor zorgen dat er ook een andere manier is om 112 te bereiken, dus ik ben heel benieuwd naar de plannen van de Minister voor die back-up. Ik ben ook benieuwd of er misschien nog andere problemen zijn dan de puur technische problemen met betrekking tot die situatie en wanneer het onderzoek naar het voorval gereed is. Want als we het over vitale infrastructuur hebben, dan hebben we het natuurlijk over 112. Dat is de meest vitale infrastructuur die we in ons land hebben.

De **voorzitter**:
Dank u wel. Dan is het woord aan de heer Middendorp van de VVD.

De heer **Middendorp** (VVD):
Dank u wel, voorzitter. Het is goed om hier te zijn. Dank ook aan de leden dat ze me de mogelijkheid geven om hier een aantal punten aan de orde te stellen. Laat ik maar meteen beginnen.
De Minister heeft aangegeven strenger te willen optreden tegen bedrijven die de veiligheid van hun eigen digitale netwerken niet op orde hebben. Ik vroeg me af hoe de Minister dit nou zelf ziet. Ik zie het wel voor me dat hij op bezoek gaat; dat maakt zeker indruk. Maar het is een heel ingewikkeld onderwerp. Gisteren heb ik bij de begrotingsbehandeling Binnenlandse Zaken een plaatje laten zien van de Rekenkamer over de cybersecurity van de overheidsnetwerken. Die is niet helemaal op orde. Het is vervelend om dit als gast te moeten opmerken, maar JenV kwam daar niet goed uit; zie pagina 39 van het Rekenkamerrapport. Dus de vraag is toch een beetje op welke basis JenV dan met de private sector in gesprek zou gaan. Dat is misschien een opening die ingewikkeld is, maar ik denk dat de sleutel ook voor een deel ligt bij coördinaties bij de overheid zelf. Daarover zijn al een aantal opmerkingen gemaakt. De samenwerking tussen de diensten en het NCSC is bijvoorbeeld volgens mij iets waar wel wat te halen valt. Ik vraag me ook af in hoeverre de Minister al gewoon in gesprek is met andere ministeries. De VVD heeft een jaar geleden een voorstel gedaan voor een rijksinspectie digitalisering, die precies ziet op meer samenwerking tussen ministeries en de uitwisseling van best practices. Ik stel gewoon een vraag: heeft de Minister al eens van dit initiatief gehoord? Want ze zijn er nu een jaar op aan het studeren bij BZK en het zou interessant zijn als dit ook al JenV heeft bereikt.
Voorzitter. Er zijn al een paar dingen gezegd over de adviserende rol die het NCSC heeft. Wat is de indruk van de Minister? Zijn die nou geëqui-

peerd om die vitale infrastructuur ook echt te helpen? Is de Minister het ermee eens dat uiteindelijk toch ook heel veel verantwoordelijkheid bij die vitale-infrastructuurinstellingen zelf zal blijven liggen? Mij viel zelf een datalek in het klachtensysteem van Schiphol op. Ik vraag me af hoe wij vanuit een ministerie dat helemaal onder controle kunnen krijgen. Hoe kijkt de Minister daartegen aan?
Voorzitter. Mijn laatste punt is: hoe ondersteunen we niet-vitale infrastructuur, bijvoorbeeld kleine ondernemingen? Ik dacht zelf ook aan cybersecurity van mensen. Laat ik beginnen met het mkb. In hoeverre is er eigenlijk een dialoog? Op welke manieren wordt de expertise van de overheid gebruikt om ook niet-overheid, marktpartijen, te helpen? Er werd al wat gezegd over het Digital Trust Center. Daar werken naar mijn informatie niet heel veel mensen: zestien mensen voor 1,3 miljoen bedrijven, als ik het goed begrepen heb. Maar ik denk dat er ook heel veel andere manieren zijn waarop de overheid, als speler in deze toch wel ingewikkelde problematiek van cybersecurity, kan helpen. Ik zal een voorbeeld geven. Er is onlangs bij het aankoopbeleid van de overheid een grote softwareleverancier vrij hard aangepakt. De informatie die daarover naar buiten is gekomen, heeft mkb'ers geholpen om hun eigen onderhandelingen met softwareleveranciers beter te kunnen voeren. Is zoiets ook denkbaar in het kader van cybersecurity?
Tot slot, voorzitter. We kunnen natuurlijk veel opleggen, adviseren en regels geven, maar uiteindelijk zijn instellingen en mensen voor een deel gewoon zelf verantwoordelijk dat ze op bepaalde punten de juiste keuzes maken. Maar er is ook nog iets als handhaving online: het opsporen van cyberoplichters, bedreigers en chanteurs, oftewel het aanpakken van digitaal tuig. Dat is een aspect van cybersecurity.

De **voorzitter**:
Wilt u afronden?

De heer **Middendorp** (VVD):
Ja, ik rond af. Ik rond af met de opmerking dat het eigenlijk gaat om meer blauw online. Hoe kijkt de Minister hiertegen aan?

De **voorzitter**:
Dank u zeer. Dan is ten slotte het woord aan de heer Van den Berge van GroenLinks.

De heer **Van den Berge** (GroenLinks):
Dank u wel, voorzitter. In een steeds meer digitaal wordende samenleving is het natuurlijk heel belangrijk om de cybersecurity op orde te hebben. Daar zullen we het allemaal snel over eens zijn. Collega Verhoeven somde terecht al een heel aantal gerenommeerde instanties op, van de WRR tot de NCTV. Het WODC noemde hij volgens mij niet, maar dat heeft ook een kritisch rapport gepubliceerd. Je kunt er een boekenkast mee vullen. Er zijn genoeg studies en harde aanwijzingen dat we de cybersecurity op dit moment onvoldoende op orde hebben. Collega Verhoeven had het al over het boek van Huib Modderkolk, dat heel inzichtelijk maakt hoe incidenten op het gebied van cybersecurity vaak het gevolg zijn van laksheid bij bedrijven. Op zich komt dat misschien wel voort uit iets heel moois: het vertrouwen in de overheid en onze veiligheid is in Nederland vrij groot. Voor een deel is dat terecht, maar als het gaat om bedreigingen op het gebied van cybersecurity dan zijn we misschien soms een tikkeltje naïef. Dat geldt trouwens ook voor ons als burgers, denk ik. Ik moet eerlijk bekennen dat ik een update van mijn software ook weleens uitstel.
Ik ben toch wel benieuwd om van de Minister te horen hoe hij dat ziet. In de media heeft de Minister inderdaad aangekondigd dat hij lakse bedrijven harder wil gaan aanpakken. Als ik vervolgens kijk naar de stukken die vandaag op de agenda staan, dan gaat het vooral over

informeren en adviseren. Dat lijkt me ook een logische eerste stap, want ik denk eerlijk gezegd dat de meeste bedrijven zelf ook de cybersecurity op orde willen hebben. Ik denk dus dat informeren, kennis delen en adviseren een logische eerste stap is. Maar zou de Minister nader kunnen ingaan op hoe de escalatieladder er wat hem betreft uitziet? Wanneer zou dat informeren en adviseren over moeten gaan in identificeren en aanpakken?
Voorzitter. Dat brengt mij op het punt van oefenen. Een aantal collega's heeft het daar al over gehad. GroenLinks denkt ook dat oefenen essentieel is om erachter te komen waar precies de kwetsbaarheden zitten in systemen, of er back-upsystemen zijn en of die op het moment suprême functioneren. Dat horen we ook vanuit verschillende sectorpartijen en het komt ook in verschillende studies, waaronder het WRR-rapport, aan de orde. In de brieven die vandaag op de agenda staan, heeft de Minister het ook over oefenprogramma's, over testen en over het scannen van vitale systemen, mede naar aanleiding van de motie van de collega's Verhoeven en Laan-Geselschap. Maar ik zou toch iets meer inzicht willen krijgen in hoe dat er concreet, in de praktijk, uitziet. Ik vind het in de brieven nog niet concreet genoeg.
Ik hoor ook vanuit het bedrijfsleven dat de laatste grote stresstest, ISIDOOR II – collega Verhoeven noemde al dat die test in 2017 heeft plaatsgevonden – tot op heden geen opvolging heeft gekregen. Ik weet niet of dat klopt, maar ik stel de vraag aan de Minister: wanneer is de laatste grote stresstest op het gebied van cybersecurity vanuit de overheid in samenwerking met het bedrijfsleven geweest? En wanneer komt daar wat de Minister betreft een vervolg op? En – deze vraag werp ik ook maar op – zou het niet logisch zijn om jaarlijks meerdere vitale systemen aan een stresstest te onderwerpen? Dat is om te kijken waar de kwetsbaarheden zitten, wat er beter moet, wat we kunnen doen op het gebied van informatie-uitwisseling om risico's af te dekken, of we extra back-upsystemen moeten opzetten? Ik kan wel even doorgaan met het rijtje vragen. Dat doe ik omwille van de tijd niet. Mijn vraag aan de Minister is dus een heel concrete: zouden we niet elk jaar een aantal grootschalige stresstesten moeten organiseren, zoals we dat op andere gebieden ook doen? Dat doen we bijvoorbeeld ook als het gaat om de veiligheid in overheidsgebouwen. Daarvoor hebben we oefeningen, waarbij we aan de hand van een zo concreet mogelijke dreiging oefenen hoe we bijvoorbeeld het pand verlaten.
Voorzitter. Dan kom ik op mijn laatste punt: Kaspersky. Ik begrijp de overwegingen van de Minister om Kaspersky uit te faseren. Maar als ik de brief van de Minister lees, en zijn overwegingen, en vooral de overwegingen die ten grondslag liggen aan het uitfaseren, waarbij het vooral gaat om de risico's die de Minister ziet komen vanuit de Russische veiligheidsdiensten die wellicht een beroep op die informatie zouden kunnen doen, dan denk ik toch ook aan 5G en Huawei. Ik weet dat de Minister eerder heeft aangegeven dat hij dat een heel andere casus vindt. Maar ik zou toch willen dat hij daar nader op ingaat, want als ik de brief over Kaspersky lees, dan klinkt het wel degelijk als een landengerichte aanpak. Als we de dreiging vanuit Rusland groot genoeg vinden om Kaspersky uit te faseren, dan ben ik toch benieuwd waarom we van 5G en Huawei niet zeggen dat we het niet zouden moeten willen en daar een stokje voor zouden moeten steken.
Hiermee rond ik af. Voorzitter, dank u wel.

De **voorzitter**:
Ik dank u zeer. Ik zie dat de Minister tien minuten nodig heeft.

De vergadering wordt van 15.29 uur tot 15.39 uur geschorst.

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

Minister **Grapperhaus**:
Voorzitter. Ik had een spreektekst voorbereid. Ik ga daar toch maar gewoon mee beginnen. Die spreektekst luidt: «Uw Kamer zal het vast met mij eens zijn dat cybersecurity als onderwerp inmiddels prominent op de agenda staat.» Ik vind cybersecurity een buitengewoon belangrijk onderwerp. Dat blijkt ook uit een aantal kritische vragen die door uw Kamerleden zijn gesteld en zorgen die zijn geuit. Daar ga ik straks op in. Maar ik vrees dat ik als verantwoordelijk en coördinerend Minister moet blijven vaststellen dat er toch wel wat ontbreekt aan dat prominent op de agenda staan. In het rapport van de WRR staat dat het vrijwel zeker is dat er een keer een groot incident komt waardoor duurzame ontwrichting ontstaat. Ik geef toe dat het verscheen toen het nog strandweer was, eind augustus, maar het heeft een minimum aan belangstelling en reacties opgewekt.
Ik zeg dat maar even zo hard, ook voor de mensen die thuis of hier in de zaal kijken, omdat cybersecurity wel degelijk een buitengewoon belangrijk onderwerp is. We hebben in deze maatschappij in heel veel gevallen geen analoge terugvalopties, en heel veel onderdelen van onze vitale infrastructuur zijn gebaseerd op digitalisering en zijn daar zelfs volledig van afhankelijk. Vandaar dat ik toch wat pinnig begin met dat ik enigszins twijfel als slechts vier van de dertien Kamerfracties die we hebben hier vandaag vertegenwoordigd zijn, met complimenten voor de fracties die er zijn. Want cybersecurity is niet alleen bespreken waar het mis gaat, bijvoorbeeld wat de heer Verhoeven terecht aanbracht: de storing die in juni bij 112 optrad. Cybersecurity – het woord security zegt het al – is dat we ervoor moeten zorgen dat onze samenleving inderdaad veilig is als het gaat om die enorme afhankelijkheid van digitale systemen en technologieën.
Voorzitter. Tot zover...

De heer **Van Dam** (CDA):
Ik wil toch wat aan de Minister vragen. Want de eerlijkheid gebiedt te zeggen dat collega Verhoeven en ik net een onderonsje hadden en eigenlijk ook zeiden: hoe kan het dat hier maar vier fracties zitten bij zo'n belangrijk onderwerp? Het is natuurlijk superfijn dat ik hier zit en dat kan zeggen, maar ergens schaam ik me daar ook voor in de richting van de Minister en alle ambtenaren enzovoort. Toch doet dat de vraag oproepen: waarom is dat dan zo? Waarom is het zo, niet alleen in de Kamer, maar ook maatschappelijk gezien, dat hier zo weinig aandacht voor is? Heeft de Minister daar een beeld bij? Als Kamer zijn we begonnen met de commissie Digitale toekomst, ook om als Kamer meer grip te krijgen op de digitale ontwikkeling, inclusief cyberveiligheid. Maar wat zou er maatschappelijk aan de hand zijn dat we daar toch kennelijk met z'n allen niet de aandacht voor hebben die we daarvoor zouden moeten hebben?

Minister **Grapperhaus**:
Het feit dat al die digitale systemen, die in het dagelijks leven heel erg met elkaar vervlochten zijn, zo goed functioneren, zit ons daar eigenlijk bij in de weg. Ons wegennet en de infrastructuur van ons openbaar vervoer zijn voortreffelijk werkende systemen en dus zult u heel zelden in de Kamer een debat krijgen over de toekomstige kwaliteit van onze geasfalteerde wegen, om maar iets te noemen. Natuurlijk komt dat in algemene overleggen wel enigszins aan de orde, maar die aandacht is eigenlijk juist zo gering doordat we het in Nederland zo goed voor elkaar hebben, waar we ook om bekend staan. Ondertussen zien we in recente tijden wel aanvallen met malware. Ik noem dat voor de mensen thuis even kwaadwillende software, die wordt ingebracht door partijen, soms ook statelijke actoren, die voor disruptie en sabotage willen zorgen. Maar we zien ook dat het meteen ontwrichtend is als er een enkele keer ergens een groot digitaal probleem ontstaat. Denkt u hierbij inderdaad aan de recente

storing bij het alarmnummer 112. Tot nu toe is het zo dat wij als Nederlanders ervan uitgaan dat de overheid het toch weer heel snel oppakt, weer heel snel de stekker in het stopcontact heeft. En wat is er dan eigenlijk aan de hand?
We moeten echter vaststellen dat die aanvallen op systemen, bij ons maar ook in andere westerse landen – denkt u even aan de twee ziekenhuizen in Engeland, maar ook aan de Rotterdamse haven in 2017 – incidenten zijn die in de toekomst in beginsel meer zullen voorkomen. Dat geldt ook gewoon voor storingen in die ingewikkelde systemen. Dat is ook waar de WRR keihard voor waarschuwt. We hebben onze maatschappij na de Tweede Wereldoorlog met elkaar heel gestructureerd en stevig opgebouwd. Als we dat ook willen in het digitale domein, dan moeten we daar echt nu, nu die incidenten zich nog nauwelijks voordoen, met elkaar scherpte in tonen en niet wachten tot er een digitale watersnood à la 31 januari 1953 plaatsvindt.
Voorzitter. Dit is de verklaring die ik toch enigszins positief aan de heer Van Dam wil geven. Ik weiger te geloven in de negatieve component, namelijk dat daar volstrekt geen interesse in zou bestaan.

De **voorzitter**:
Er is een interruptie van de heer Van Dam. Houd het kort graag.

De heer **Van Dam** (CDA):
Ja, dat zal ik doen. Ik was onlangs, waarvoor dank nog, op werkbezoek bij het NCSC en toen hadden we het over voorspelbaarheid en voorstelbaarheid. Je kunt bepaalde dingen voorspellen. Maar kun je je die ook voorstellen? In dat boek dat hier al genoemd is, van de Volkskrantjournalist, wordt bijvoorbeeld gesproken over of je als Nederlander niet een paar honderd euro in huis moet hebben voor het geval er een langdurende pinstoring is. Hoe ga je je boodschappen halen als je niet meer kunt pinnen? Dan kom je ook op het punt van voorstelbaarheid. Kun je je voorstellen dat dat gebeurt? Dat is ook de reden waarom ik zo hamer op het betrekken van de burger bij dat hele verhaal van cyberveiligheid. Zou de Minister daar nog eens op willen reageren? Hoe kunnen we organiseren dat de voorstelbaarheid van dit soort dreigingen bij burgers, bij mensen zoals u en ik, toeneemt? Want daar zit volgens mij een crux.

Minister **Grapperhaus**:
Ik denk dat het scherp en groots opzetten van publiekscampagnes daarbij zeker zou moeten kunnen helpen. Het heeft ons geholpen om de high-impact crimes terug te dringen, de diefstallen, roofovervallen en dergelijke. Een campagne tegen cybercrime heeft ons hopelijk ook geholpen. Dat gaat we het komende jaar pas echt zien. Daar kom ik nog op terug. Dat betrof de campagne – ik heb het hier staan – «eerst checken, dan klikken». U ziet dat ik dat menigmaal gedaan heb, zo goed dat ik het uit het hoofd weet. Nu kom ik toch weer op iets symbolisch: vroeger had iedere Nederlander in zijn trapgat, of onder zijn keldertrap, 40 conservenblikken staan. Het zou me heel erg benieuwen hoeveel Nederlandse huishoudens dat nog hebben voor de situatie dat zich voedselnood voordoet. Respectievelijk vraag ik me af hoeveel Nederlandse huishoudens toch nog bijvoorbeeld een vaste telefoon hebben, voor het geval het mobiele netwerk van deze of gene uitvalt. U ziet, en dan houd ik erover op, dat als een bepaalde provider besluit om zijn netwerk om te zetten via Duitsland, iedereen meteen in alle staten is. Daar kan ik, als verantwoordelijk Minister, nog enigszins om glimlachen, want dat was omdat het internet daardoor trager werkte. Maar we hebben gezien met de stroomstoring in Amsterdam van enkele jaren geleden dat het echt van het grootste belang is dat de diensten dan op tijd kunnen handelen, dat mensen niet nodeloos alarmnummers gaan bellen en dat mensen toch een zekere weerbaarheid hebben op «het kan gebeuren».

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Nu ik de heer Van Dam toch al van repliek diende, wil ik zeggen dat het me het beste lijkt om per Kamerlid, te beginnen met de heer Van Dam, de vragen te beantwoorden. De heer Van Dam had natuurlijk terecht een heel prangende vraag. Hij vroeg zich af: wie heeft toch bedacht dat het de Wet beveiliging netwerk- en informatiesystemen zou moeten gaan heten? Want ieder kind kan toch bedenken dat de Cybersecuritywet in ieder geval dat begrip goed in de huishoudens naar binnen gooit? Er zijn momenten dat ik word overvallen door een geweldig geheugenverlies, maar ik weet zeker dat de heer Van Dam op de persconferentie, die straks vermoedelijk ook door één journalist bezocht wordt, nog eens kan uitleggen waar de naam Wet beveiliging netwerk- en informatiesystemen vandaan komt. Als troost voor al die burgers die gek worden van zo'n ontzettend lange, omslachtige, niet goed duidende naam van de wet – die burgers zouden naar ik begrepen heb zonder enige twijfel via Facebook, of een ander cybertechnisch communicatiemiddel, een petitie om het alsjeblieft de Cybersecuritywet te noemen door een miljoen mensen ondertekend kunnen krijgen – wijs ik u op het Cybersecurity Woordenboek. Dat is nog ouderwets op papier uitgegeven. Dus mocht uw app uitvallen; u kunt dit Cybersecurity Woordenboek onder de zoldertrap gelegd hebben, naast de blikken met bonen en erwten. Dat boek geeft een hele verklarende woordenlijst van alles wat plaatsvindt. Omdat mij is gebleken dat het boek in de winkel minder dan € 50 kost, heb ik gemeend uw leden, voor zover thans aanwezig, als beloning voor die aanwezigheid een exemplaar te mogen aanbieden. Als daar bezwaren tegen zijn dan hoor ik dat graag.
Voorzitter. Dan ga ik over op de andere vragen van de heer Van Dam. De heer Van Dam stelde een belangrijke vraag. Dat Nationaal Cyber Security Centrum zit in het Ministerie van Justitie en Veiligheid. Dat is eigenlijk het orgaan dat vitale organisaties bijstaat met informatie, maar het informeert en adviseert ook als er sprake is van digitale dreiging of incidenten. Dat doet men gericht voor de eigen partners, en daarnaast worden door het NCSC, zoals ik het verder zal aanduiden, openbare adviezen met zogenaamde handelingsperspectieven gegeven, zodat men weet wat bepaalde situaties zouden kunnen betekenen en wat er moet gebeuren. Ik ga straks nog in op de vraag van de heren Van Dam en Middendorp over wat dat nu eigenlijk betekent voor de gewone burger. Dat kan ik eigenlijk nu ook wel zeggen. Wat doen we daarvoor? Daar worden ook campagnes voor ontwikkeld. Ik wees al op «eerst checken, dan klikken». U heeft die spotjes ongetwijfeld op tv en sociale media voorbij zien komen. Die zijn er vooral op gericht om de oplettendheid van mensen op cybercrime te vergroten. We hebben het hierbij over zaken als phishing. Die campagne wordt straks voortgezet en gaat zich dan richten op de veiligheid van de internet-of-thingsapparaten. Ik mag graag het voorbeeld aanhalen van thermostaten die je op afstand kunt bedienen. Die worden vanuit de fabrikanten – laat ik in algemene zin spreken – niet altijd met voldoende beveiliging geleverd, met als risico dat die apparaten makkelijk te hacken zijn. Nou is een hack van één thermostaat nog tot daar aan toe, maar het internet of things zou ook in heel groten getale kunnen worden gehackt door een kwaadwillende partij. Dan moeten we er niet aan denken dat de apparaatjes van 30.000 huishoudens in het midden van de winter, veronderstellende dat de winter ondanks de klimaatverandering voorlopig nog wel doorgaat in ons land, ineens worden gemanipuleerd en dat mensen die kwetsbaar zijn zodanig in de kou kunnen komen dat er bijvoorbeeld 's nachts ongelukken gebeuren.
Daarnaast hebben we ook aandacht voor slachtoffers. Slachtofferhulp Nederland heeft een nieuw onlineplatform gelanceerd met specifieke

informatie voor slachtoffers van onlinecriminaliteit. Het is goed om daar hier even aandacht op te vestigen. Mijn collega Sander Dekker, Minister voor Rechtsbescherming, heeft de Kamer daar in februari op geattendeerd.
En dan is er de versterking van de opsporing. Op 1 maart van dit jaar is de Wet computercriminaliteit III van kracht geworden. Dat is een wet met een heel krachtige, verhelderende naam, zou ik haast willen zeggen. Daarin is niet alleen de bevoegdheid tot het binnendringen in een geautomatiseerd werk opgenomen, maar ook de strafbaarstelling van het stelen en helen van gegevens en van onlinehandelsfraude. Want laten we wel wezen, ook dat zijn allemaal aspecten van cyberinsecurity, zoals ik het maar zal noemen.
Overigens is ook met dat wetsvoorstel de inzet van de lokpuber mogelijk gemaakt om misdrijven op het terrein van misbruik van kinderen en jongvolwassenen beter te kunnen aanpakken. U denkt misschien: dat is dan toch weer net even een heel andere tak. Maar ik noem dat even, omdat het allemaal voorbeelden zijn van wat ik cyberinsecurity noem, die zich steeds meer voordoen en waar we als maatschappij steeds meer tegen gewapend moeten zijn.

De heer **Middendorp** (VVD):
De Minister begon met de vraag van de heren Van Dam en Middendorp over mensen. Het antwoord ging over weerbaar zijn et cetera. Ik weet niet of het stukje over handhaving nog komt, waar ik naar vroeg, maar anders zou mijn vraag zijn...

Minister **Grapperhaus**:
Dat komt zo

De heer **Middendorp** (VVD):
O, pardon. Excuus.

Minister **Grapperhaus**:
Ik doe het per Kamerlid. Dat is voor de kijkers en voor de mensen in de zaal iets minder systematisch, maar gezien de hoeveelheid Kamerleden leek mij dat in dit geval het meest opportuun.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
De heer Van Dam vroeg hoe het zit met de toezichthouders in de diverse sectoren. Diverse sectoren hebben hun eigen cybertoezichthouder. Hebben die voldoende kennis? De toezichtrol op het gebied van cyber is inderdaad voor sommige van die toezichthouders gewoon nieuw. Dat zijn dan vaak inspecties van ministeries. Ze zijn sinds dit jaar aangewezen onder de Wet beveiliging netwerk- en informatiesystemen, dus de Wbni. Ze moeten dus nog groeien in die taak. Dat valt niet te ontkennen. Er vindt veel onderlinge kennisuitwisseling plaats en de NCTV, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, en de Inspectie JenV, de inspectie van het Ministerie van Justitie en Veiligheid, staan die toezichthouders ook bij met informatie en kennis.
Voorzitter. Het is belangrijk om hier te melden – dat staat ook in mijn brief aan uw commissie van gisteren, aan uw Kamer – dat alle betrokken toezichthouders op dit moment, onder leiding van de Inspectie Justitie en Veiligheid, een eerste rapport maken van hun bevindingen. Dat geeft daarmee ook een gezamenlijk beeld. Ik denk dat dit een heel goede ontwikkeling is, want dat is een verdere stap naar volwassenheid van die toezichthouders.

Dan kwam ook de vraag van de heer Van Dam over de meer tastbare verantwoording dan nu in het Cybersecuritybeeld Nederland voorkomt. Ik begrijp dat punt zeer. Dat Cybersecuritybeeld Nederland laat op hoofdlijnen zien hoe het ervoor staat met de digitale dreiging en weerbaarheid in Nederland, maar je moet ook een vertaling hebben naar tastbare en concrete maatregelen. Ik kom later nog met wat voorbeelden, maar ik ben het in ieder geval met hem eens dat we een zo concreet mogelijk beeld nodig hebben. Daarom bijvoorbeeld ook dat inspectiebeeld waar ik het net al over had, zodat men niet alleen weet wat de normen zijn waaraan voldaan moet worden, maar dat men ook echt ziet waar het niet goed gaat en waar wat moet worden opgepakt.
Voorzitter. Ik citeer even uit het door ik meen de heer Middendorp – maar het kan ook de heer Verhoeven zijn geweest, excuus daarvoor – naar voren gebrachte rapport van de Algemene Rekenkamer, waarin je ziet dat delen van onze vitale infrastructuur nog steeds draaien op 2G. Ik zou bijna, met een verwijzing naar een diskjockey uit mijn jeugd, willen zeggen: herinnert u zich deze nog? Dat zijn natuurlijk heel concrete punten die je aan overheden of aan delen van het bedrijfsleven die in onze vitale infrastructuur zitten, kunt laten zien. Zo van: luister eens, dat zijn dingen die je nu echt moet brengen naar de nu geldende standaarden.
Maar het gaat ook om concrete maatregelen op het gebied van het aanspreken van producenten die inderdaad in groten getale internet-of-thingsapparaten aanleveren, want het alleen aanspreken van de consumenten zal niet de volledige oplossing zijn.
Ik heb al gezegd dat het NCSC vitale organisaties bijstaat met informatie. Het is wat dat betreft echt de vraagbaak en de centrale draaischijf als het gaat om het in concrete gevallen vertalen van dat Cybersecuritybeeld Nederland, ook als het een keer wat abstracter is, naar adviezen over welke maatregelen bedrijven zouden moeten nemen.
De heer Van Dam vroeg ook naar het Digital Trust Center.

De heer **Van Dam** (CDA):
Toch nog even over die concretere verantwoording. Wij hebben een prachtige Cybersecurity Agenda met zeven domeinen gekregen van het kabinet. Ik heb hier zelfs nog een versie met bullets enzovoorts, want ik houd heel erg van korte overzichten. Toch is mijn vraag aan de Minister: ik zou graag de voortgang van die zeven punten in beeld willen hebben. Ik denk dat de verantwoording op dat Cybersecuritybeeld meer betrekking heeft op eventualiteiten die zich in de werkelijkheid voordoen, zoals bedreigingen enzovoorts. Ik wil meteen graag even van de gelegenheid gebruikmaken. De Minister had het er net over dat er zo weinig aandacht is voor het WRR-rapport. Alleen is het dacht ik vooralsnog niet naar de Kamer gestuurd. Of heeft u gezegd dat u nog met een beleidsreactie komt?

Minister **Grapperhaus**:
Dat laatste.

De heer **Van Dam** (CDA):
Dat laatste. Dus wat dat betreft is het ook niet zo heel raar dat wij er hier nog niet over hebben gesproken. Ik vond dat toch wel fijn om even te zeggen.

De **voorzitter**:
Goed. Dan resteert het antwoord op de eerste vraag over de voortgang.

Minister **Grapperhaus**:
Ik proefde bij die tweede toch ook een soort stil vraagteken. Maar wat dat eerste punt betreft kan ik tegen de heer Van Dam zeggen dat we volgend jaar – dat gaat in de jaren erna steeds zo – naar aanleiding van het

Cybersecuritybeeld Nederland aangeven hoe de ontwikkeling is van die zeven punten die u net noemde. Dus we gaan daar inderdaad een voortgezet beeld maken. In wezen is die, ik zou haast willen zeggen, schijf van zeven die u daar heeft een soort nulmeting op dat punt. Dus ik kan u bij dezen toezeggen dat dit gaat gebeuren.

De heer **Van Dam** (CDA):
Zou ik dan nog heel kort mogen horen wanneer dat volgend jaar ongeveer wordt gedaan? Want het jaar duurt denk ik ook weer 365 dagen.

De **voorzitter**:
366 zelfs.

Minister **Grapperhaus**:
Ja, volgend jaar hebben we 366 dagen. Zal ik daar ook nog over uitweiden?

De **voorzitter**:
Nou, als u zou willen? Graag.

Minister **Grapperhaus**:
Dat is de caesarische kalender, maar dit geheel terzijde. Dat zal nog zijn in het voorjaar, waarbij ik er wel op wijs, voor degenen die dat niet meer wisten als gevolg van de digitalisering, dat het voorjaar loopt tot en met 20 juni. Maar ik verwacht dat we in de eerste helft van juni, maar zeker dus nog in het voorjaar, bij uw Kamer zullen terugkomen op de voortgang of achteruitgang, of hoe u het wilt noemen, van die schijf van zeven uit de Cybersecurity Agenda.

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

Minister **Grapperhaus**:
Voorzitter. Dan nog even dat stille vraagteken. Ik wil tegenover uw commissie benadrukken dat ik het feit dat wij hier deze discussie hebben in ieder geval erg goed vind. Van dat WRR-rapport heb ik gezegd dat het nauwelijks weerklank heeft gekregen, niet in de publiciteit en ook niet in gesprekken tussen uw Kamer en mij. Ik realiseer mij dat de beleidsreactie nog niet rond is, maar ik blijf hier als refrein herhalen dat het rapport gewoon keihard zegt: an accident is waiting to... Pardon, het moet in het Nederlands: er staat gewoon een ongeluk, een groot incident, te gebeuren dat voor duurzame ontwrichting gaat zorgen.
Voorzitter. De heer Van Dam vroeg of het vertrouwelijke inspectiebeeld deelbaar is. We gaan die bevindingen meenemen in het Cybersecurity-beeld Nederland. Maar het is nu nog te vroeg om aan te geven in hoeverre dat beeld tot op vertrouwelijkheidsniveau kan worden gedeeld, want we zullen bij cybersecurity ook te maken hebben met uiterst vertrouwelijke informatie die onze infrastructuur betreft. We kunnen dat natuurlijk niet allemaal delen.
Dan had ik ten slotte nog de vraag van de heer Van Dam over de kennis bij de toezichthouder. Nee, die heb ik besproken. Dus dan heb ik als het goed is de vragen van de heer Van Dam besproken en kom ik bij de heer Verhoeven.
De heer Verhoeven wees nog eens op de kwestie van de Pulse VPN en de doorzettingsmacht. Hoe gaan we nou die rol van het NCSC, het Nationaal Cyber Security Centrum, verbeteren? Het NCSC speelt een centrale rol in het stelsel. Zoals gezegd, werkt het dus samen met die sectorale toezicht-houders. Zij worden door de concrete dreigingsinformatie in positie gebracht. Het NCSC is ook degene die toezicht houdt op de digitale weerbaarheid in de verschillende sectoren. U weet dat we daar nog iets

uitvoeriger over hebben gesproken naar aanleiding van een mondelinge vraag van enige tijd geleden over die Pulsekwestie. Volgens mij was dat een vraag van de heer Van Raak van de SP. Die sectorspecifieke kennis maakt dat het NCSC ook goed kan beoordelen of een organisatie de juiste beveiligingsdoelen nastreeft. «De juiste beveiligingsdoelen» wil zeggen dat de organisatie het gewenste beveiligingsniveau heeft.
Een benadering die in dit kader binnen het domein van cybersecurity effectief werkt, is het beschrijven van beveiligingsdoelen met daaraan gekoppeld bepaalde beheersmaatregelen. Vertaald naar de fysieke wereld betekent dit bijvoorbeeld dat de toezichthouder als beveiligingsdoel stelt dat indringers niet in een bepaalde kamer mogen komen. Maar de toezichthouder zegt niet dat er een slot op de deur moet komen, want dat is natuurlijk uiteindelijk de beslissing die je zelf moet nemen om ervoor te zorgen dat die indringers niet in die bepaalde kamer mogen komen. Als we dat naar digitale systemen of delen daarvan vertalen, dan zie je daar dus hetzelfde. Men stelt vast dat iets een heel vitaal, maar kwetsbaar deel van je systeem is en dat je dat echt goed in de cybersecurity moet hebben. Dan kan men eventueel nog suggereren wat daar de middelen en methodes voor zijn, maar de verantwoordelijkheid voor hoe dat wordt opgepakt, is natuurlijk aan de betrokken partijen en de vakdepartementen in die vaksectoren zelf.
Voorzitter. De heer Verhoeven vroeg hoe het staat met de voortgang van zijn motie over de kwetsbaarhedenscan van de vitale infrastructuur. Aan die motie wordt op dit moment hard gewerkt door mijn collega van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dat Ministerie van BZK verkent de mogelijkheden voor het inrichten van een gezamenlijke geautomatiseerde scanfaciliteit voor alle rijksdiensten. Men werkt momenteel bijvoorbeeld aan het instellen van kaders voor het scannen naar kwetsbaarheden als tussenstap. De Nationaal Coördinator Terrorismebestrijding en Veiligheid, de NCTV, en het Nationaal Cyber Security Centrum, het NCSC, zijn in een adviserende rol betrokken bij het ontwikkelen van die geautomatiseerde scan.
Vorige week heeft mijn collega van Binnenlandse Zaken en Koninkrijksrelaties uw Kamer over deze rijksbrede faciliteit geïnformeerd in de voortgangsbrief – ik noem hem nog maar even – Strategische I-agenda. Op basis van de ervaringen bij het Rijk wordt dan bezien in welke mate die methodiek kan worden toegepast bij de bredere vitale infrastructuur. Daarnaast wordt op allerlei manieren gewerkt aan het vergroten van inzicht in kwetsbaarheden in de vitale infrastructuur, dus het vergroten van het inzicht in die kwetsbaarheden zelf. Dat gebeurt onder meer door oefen- en testprogramma's.
De heer Verhoeven vroeg of zo'n Pulseachtige patch onder de zorgplicht van de Wbni zou vallen en of er dan ook boetes kunnen worden uitgedeeld. De zorgplicht van de Wbni stelt dat aanbieders van een essentiële dienst en digitale dienstverleners passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen en incidenten te voorkomen en beheersen. Het doel van die zorgplicht van de Wbni is dus het waarborgen van de continuïteit van hun dienstverlening.
Onderdeel is bijvoorbeeld een maatregel die ziet op het inrichten en onderhouden van een volwassen niveau van patchmanagement in een organisatie. Daar houden toezichthouders toezicht op. Het uitvoeren van updates en patches is iets wat dagdagelijks plaatsvindt in een organisatie. Ik geef toe dat het woord dagdagelijks me wel enigszins doet denken aan het woord topprioriteit. Volgens mij zeg je twee keer hetzelfde, maar goed. Individuele patches maken als zodanig onderdeel uit van die brede maatregel van patchmanagement.
Als uit bevindingen van de toezichthouder naar voren komt dat het patchmanagement of andere onderdelen van de zorgplicht van onvoldoende niveau zijn, dan zal het NCSC een organisatie bewegen om dat te

verbeteren en toezien op de naleving van die verbetering. Als dat nog steeds niet lukt, dan beschikt de toezichthouder over diverse interventiemethoden waaronder ultimo boetes. Op dit moment heeft het Agentschap Telecom geen boetes uitgedeeld, aangezien men daar niet het beeld heeft dat bij de onder hem toezicht vallende organisaties sprake is van nalatigheid ten aanzien van de zorgplicht en de processen voor patchmanagement.
Maar dan komen we natuurlijk toch op het punt waar de heer Verhoeven terecht zijn vragen op toespitst, namelijk welke stappen de Minister gaat zetten, kijkend naar de paraatheid of eigenlijk de zorgen daarover die worden genoemd in het WRR-rapport. Ik kom begin volgend jaar met een kabinetsreactie waarin ik dat uitgebreid zal toelichten. Ik heb al eerder aangegeven, ook in reactie op vragen bij interruptie van de heer Verhoeven, dat ik dat punt zeer serieus neem. Ik kom in ieder geval begin volgend jaar met het nationaal crisisplan ICT, waarmee we ons nou juist op dit soort incidenten voorbereiden. Het lijkt het wel alsof we dat schrijven in reactie op het WRR-rapport, maar dat is niet zo. Er werd al gewerkt aan het nationaal crisisplan, maar het is inderdaad ook meteen een antwoord op de vragen en zorgen van de WRR, de Wetenschappelijke Raad voor het Regeringsbeleid. Ik realiseer mij nu dat ik dat even moet duiden voor degenen die dat misschien niet helemaal voor de geest hadden. Een onderdeel van de voorbereiding is ook het verhogen van de digitale weerbaarheid. Dat doe ik met de door mij aangekondigde stappen in het kader van de versterking.
De heer Verhoeven had ook vragen over het onderzoek naar 112. Dat loopt nog op dit moment. Ik zal op afzienbare termijn een voortgangsgesprek hebben met de vertegenwoordigers op het niveau van de raad van bestuur van KPN, in ieder geval de mensen die daar echt op het hoogste niveau van de raad van bestuur zitten. Ik verwacht eigenlijk dat dat onderzoek niet al te lang meer op zich zal laten wachten.
De heer Verhoeven vroeg nog wanneer de volgende cybercrisisoefening is. U had letterlijk gevraagd wanneer de volgende ISIDOOR is, maar ik vertaal het voor de mensen thuis even als de eerstvolgende cybercrisisoefening. ISIDOOR 2020 is de grootschalige cybercrisisoefening in Nederland. De doelgroep daarvan bestaat uit rijksoverheid, vitale aanbieders en partijen die een belangrijke rol vervullen ten tijde van cybercrises in Nederland. Die oefening wordt in 2020 voor de derde keer georganiseerd onder auspiciën van mijn ministerie. Daarmee wordt het nationaal crisisplan digitale ontwrichting, dat vroeger het nationaal crisisplan ICT heette, geoefend. Ik hecht zeer veel waarde aan die oefening. Ze draagt bij aan de voorbereiding van Nederland op situaties waarbij sprake kan zijn van digitale ontwrichting. U hebt het mij een aantal keren horen zeggen en ik zeg het echt niet om paniek te genereren, maar we moeten nu echt met elkaar gealerteerd zijn op wat de WRR heel duidelijk heeft aangegeven. Zo'n incident dat tot algehele digitale ontwrichting leidt, is een ongeluk dat staat te gebeuren.

De heer **Verhoeven** (D66):
We hebben een rapport van de WRR over digitale ontwrichting en paraatheid. De Minister zegt: ik kom begin volgend jaar met een reactie daarop. Dat is vier maanden later. Iets later zegt hij: het 112-onderzoek komt binnen afzienbare tijd; het duurt niet al te lang meer. We hebben het over digitale ontwrichting en 112, waarbij zich een concrete dreiging en een concreet probleem hebben voorgedaan. Het kabinet zegt: daar gaan we binnen nu en een paar maanden op reageren. Dat vind ik geen termijn die recht doet aan de ernst van de situatie. Ik vind wel dat de woorden van de Minister recht doen aan de ernst van de situatie, maar ik vind de handelingssnelheid waarmee het kabinet op deze twee concrete zaken ingaat, aan de trage kant. Kan de Minister daar een reactie op geven?

Minister **Grapperhaus**:
Laat ik beginnen met de heer Verhoeven hopelijk enigszins gerust te stellen, zodat het niet een misverstand is. Het nationaal crisisplan komt al eind dit jaar. De kabinetsreactie op het WRR-rapport komt begin volgend jaar. Ik realiseer me dat ik misschien twee keer «begin volgend jaar» heb gezegd, maar dat is niet helemaal juist. Het een komt eind dit jaar en het ander komt begin volgend jaar. Dat is één.
Twee. De heer Verhoeven en ik hebben in de Tweede Kamer al eerder met elkaar gesproken over 112. Wij kwamen tot de voorlopige conclusie dat ook onderzocht moet worden in hoeverre een dergelijk systeem bij meer dan een partij zou moeten draaien. Dat is één. Dat is iets wat ook in het onderzoek wordt meegenomen. Dan moet je ook kijken naar wat dat weer voor consequenties heeft. Mij is bekend dat KPN in de openbaarheid heeft gezegd dat men dat misschien ook een goed idee vindt. Ja, tot uw dienst dat een leverancier op enig moment zegt «misschien moet er maar iemand bij komen», maar dan moeten we wel kijken wat dat voor andere effecten heeft. Bovendien: wat zijn dan de kostenaspecten die daarin meespelen en dergelijke? Ik weet dat het primair om de veiligheid gaat, maar toch. Ik heb expres genoemd dat ik binnenkort weer een voortgangsgesprek heb met het bestuur van KPN. Ik kan de inspectie die dat onderzoek doet, niet onder druk zetten, maar ik streef er echt naar dat men de mogelijkheid heeft om zijn rapporten zo spoedig mogelijk af te ronden.

De heer **Verhoeven** (D66):
Ik begrijp dat dat nationaal crisisplan al gaande was voordat de WRR met zijn signaal kwam, dus ik ben blij dat dat eind december komt. Wat ik nu zeg, doet misschien niet helemaal recht aan de realiteit, maar zo'n groot ministerie met zo veel slimme ambtenaren moet toch in staat zijn om binnen een paar weken op zo'n rapport van de WRR te reageren? Dat lijkt mij toch echt wel tot de mogelijkheden behoren. De Minister moet maar voor lief nemen dat ik dat zeg, want dat vind ik wel.
Wat betreft KPN, 112, het back-upsysteem en een tweede partij erbij: ik heb inderdaad ook in het openbaar gehoord dat KPN dat een denkbare gedachte vindt. Ik heb het zelf geopperd. Er zijn meer partijen die hebben gezegd: het is toch heel raar dat KPN de enige toegang tot 112 is? Is dat onderzoek erop gericht om dat te veranderen of wordt er in dat onderzoek ook nog naar andere aspect gekeken? Het is misschien te smal om het alleen te beperken tot de «back-up/één provider»-vraag, maar misschien ook niet. Dat weet ik niet. Ik weet niet wat de onderzoeksvraag is. Waar gaat het onderzoek precies om? Het lijkt me sowieso logisch dat een tweede of een derde provider ook toegang tot 112 krijgt. Dat heeft de situatie die heeft plaatsgevonden, namelijk al uitgewezen, dus daar hoef je geen onderzoek meer naar te doen.

Minister **Grapperhaus**:
Laat ik met dat laatste beginnen, dus met dat onderzoek. Ik ben terughoudend om «sowieso» – in het Nederlands «hoe dan ook» – te zeggen, want ik vind dat je een onderzoek in ieder geval open-minded moet aangaan. Daarom haalde ik aan – dat weet de heer Verhoeven ook – dat KPN zelf vrij snel zei: dat moet misschien voortaan maar door meer partijen gedaan worden. Maar ik wil niet in het onderzoek de bias krijgen dat het misschien wel daardoor is gekomen. Ik hoop dat ik daarmee ook meteen het andere deel van deze vraag van de heer Verhoeven beantwoord. Een bias is trouwens een vooroordeel. De tweede vraag is of je dit door één partij laat doen of door meer partijen. We onderzoeken primair wat er gebeurd is, hoe het komt en wat we daar voor lering uit kunnen trekken. Zoals gezegd, is wat mij betreft een tweede vraag: moeten we dan kijken of we dat als remedie voortaan met meer partijen zouden moeten doen? Nogmaals, ik wil echt benadrukken dat ik daarbij uiteraard

afhankelijk ben van de input die KPN geeft vanuit diens eigen bevindingen, maar ook van wat mijn inspectie en het Agentschap Telecom nu precies vaststellen. Maar de heer Verhoeven en ik kennen elkaar zo goed – tenminste, dat hoop ik – dat hij weet dat ik, waar dat binnen de grenzen van onafhankelijkheid en onpartijdigheid mogelijkheid is, uiteraard wel nastreef dat voortvarendheid wordt betracht.
Het WRR-rapport. De gemiddelde reactietijd op een WRR-rapport is zes maanden. Laat ik daarmee beginnen. Dat betekent dat wij al bezig zijn om die tijd te verkorten. Nou is dat nog niet alles, want ik deel het gedachtegoed van de heer Verhoeven: dit is urgente problematiek, daar moeten we niet te lang mee wachten. De problematiek daarbij is wel dat dit de input van een aantal andere departementen vergt. Ik neem de complimenten aan mijn ambtenaren voor hun intelligentie en werklust dus weliswaar in ontvangst – ik kan slechts bevestigen dat die complimenten zeer terecht zijn – maar ik beloof dat ik er echt achterheen zit dat we dat meteen in het begin van het jaar hebben. Wat mij betreft kunnen wij daar snel met uw Kamer over in gesprek, want het is een belangrijk en urgent rapport. Daar ben ik van doordrongen.

De heer **Verhoeven** (D66):
Dank voor de antwoorden. Nog één wat meer procedureel punt. Volgens mij wordt binnenkort in de Tweede Kamer een wet behandeld die heel erg raakt aan deze problematiek. Is het onderzoek dat door de inspectie wordt gedaan voor de behandeling van die wet beschikbaar? Anders zou er weleens een omissie kunnen optreden doordat we de wet over de meldkamers gaan behandelen. Volgens mij staat dat voor ergens in december gepland. Dat raakt echt wel heel nauw aan de problematiek met 112 en het inspectierapport.

Minister **Grapperhaus**:
Ik moet me wel even afvragen of die twee echt aan elkaar raken. Dat vraag ik mij zeer af. Daar wil ik in de tweede termijn nog uitvoerig op terugkomen. Het staat mij bij dat ik bij de voorbereiding van de behandeling van die wet een soortgelijke vraag heb gesteld en dat dit toch niet aan elkaar raakt. Maar ik beloof u daar zo nog even duidelijk op terug te komen. Heel soms moet ik het ook even conform de aloude quiz opzoeken.
Voorzitter. Dan hebben we nog ISIDOOR III. Ik wil benadrukken dat ik die als zeer belangrijk zie. De komende maanden gaan de voorbereidingen voor het doen van ISIDOOR gezwind door, en dan niet met een verouderd plan, maar echt met het plan dat is aangepast naar aanleiding van de update van het nationaal crisisplan inzake digitale ontwrichting.
En dan het onderzoek naar benodigde investeringen. Ik ga weer mijn aloude «Inspector Columbo»-methode toepassen en dat is: meteen aan het begin van de aflevering de plot vertellen. Ik zeg dat onderzoek dus zonder meer toe aan de heer Verhoeven. Dan komen nog 50 minuten met wat uitleg; die wil ik beperken door te zeggen dat ik het geheel met Verhoeven eens ben dat we op tijd werk moeten maken van het in kaart brengen van nieuwe maatregelen en de daarbij behorende investeringen. De vraag van de heer Verhoeven stelt nou net aan de orde waar het om gaat. Daarom zeg ik dat onderzoek zo graag toe. We moeten in die urgentie ook zeggen waar we de komende jaren naartoe moeten, wat we moeten organiseren en wat dat gaat kosten. Kortom, wat hebben we daarvoor nodig? Overigens heb ik ook nog gezegd dat ik in 2021 met de overkoepelende evaluatie van de nationale cybersecurityagenda ga komen. Dat staat dus even los van de jaarlijks terugkerende voortgang in de «digitale schijf van zeven», zal ik maar zeggen.
Voorzitter. Dan kom ik bij de heer Middendorp. De allereerste vraag die ik wil beantwoorden is of ik gehoord heb van het initiatief van BZK over de samenwerking van diensten en het NCSC. Er wordt op diverse vlakken

nauw met elkaar samengewerkt, zowel operationeel als strategisch. Dat gebeurt in het kader van de nationale veiligheid doorlopend, op initiatief van zowel Binnenlandse Zaken en Koninkrijksrelaties, als het onder mij ressorterende NCSC, als de collega's van Defensie. Dat initiatief wordt hierbij dus bevestigd, evenals mijn bekendheid daarmee en mijn betrokkenheid daarbij.
De heer Middendorp vroeg verder in hoeverre we nou in gesprek zijn met andere departementen. Over de Wet beveiliging netwerk- en informatiesystemen, voorheen Cybersecuritywet, ben ik doorlopend met mijn collega's in gesprek, want die wet ligt echt aan de basis van onze cybersecurityaanpak. Daarin vindt u de middelen die we hebben. Daar kom ik zo nog wel kort op terug, want de heer Middendorp heeft ook een vraag gesteld over het ingrijpen en dergelijke. Daar geeft die wet al belangrijke instrumenten voor. In het vragenuur van begin september – het was ergens in september; het precieze moment ben ik even kwijt – heb ik gezegd dat het erg belangrijk is dat we komen met een heel duidelijke autoriteit met doorzettingsmacht. Met mijn collega's van andere departementen ben ik nog in gesprek – dat heeft u in de brief van gisteren kunnen lezen – over de manier waarop we dat precies vorm moeten geven. Ik wil wel verklappen dat ik vind dat dat niet weer een nieuwe instantie zou moeten zijn, maar dat dat bij voorkeur in de zeer directe omgeving van het NCSC zou moeten liggen.
De heer Middendorp vroeg ook naar de handhaving online. Er is een Team High Tech Crime bij de Nederlandse politie. Dat is een zeer gespecialiseerd team. Ik zou uw commissie bijna willen aanmoedigen en misschien zelfs willen uitnodigen om een keer bij dat team in Driebergen langs te gaan, voor zover u dat nog niet heeft gedaan. Gezien het aantal leden van de commissie op dit moment zou u om daarnaartoe te gaan niet eens een busje hoeven huren, laat staan een grondverzetmachine. Als de heer Middendorp daar gaat kijken, zal hij zien dat men daar inmiddels echt hele grote slagen heeft gemaakt op het gebied van opsporing van cybercrime in heel verschillende vormen, waar ik in mijn inleiding bij de eerste vraag over gesproken heb.
Dan de belangrijke vraag van de heer Middendorp hoe ik ga ingrijpen bij bedrijven. Laat ik vooropstellen: het gaat niet alleen om bedrijven, maar ook om de publieke sector. Ik ben daar heel open over. De heer Middendorp wijst er terecht op dat er ook bij diverse ministeries, ook bij mijn ministerie, zaken nog lang niet op orde zijn. Helaas is dat voor mij geen reden voor een milde glimlach, want ik vind dat totaal niet goed. We zetten erop in om dat op orde te brengen. Bij de vraag hoe ik ga ingrijpen is het heel belangrijk om de nuance mee te geven die ik aangaf in een interview in Het FD, waar de heer Middendorp aan refereerde. Ik heb toen gezegd: dit wordt niet een soort A-Team. We gaan niet de situatie krijgen dat er mensen met digitale gereedschapskisten binnenstormen die zeggen: wij gaan het nu wel even doen. Dat is juridisch niet mogelijk, maar ik vind dat ook onwenselijk, want we moeten – dan kom ik terug op het punt van de weerbaarheid – de verantwoordelijkheid ook bij de bedrijven en de burgers zelf leggen. Net zo goed als je er vroeger bij een analoge brug voor moest zorgen dat je kwartje in het klompje van de brugwachter kwam en je niet kon zeggen «ik kon er niets aan doen, want hij hield het klompje er niet goed bij», moet je er, op het moment dat het vliegwiel van cybersecurity op gang is gekomen, als bedrijf of burger in deze digitale wereld nu zelf achterheen gaan.
Verder moeten we natuurlijk ook vaststellen dat het voorlopig alleen gaat om de aanbieders van essentiële diensten. Dat zijn de organisaties die zo belangrijk zijn voor de continuïteit van de samenleving dat uitval geen optie is. Vergelijk het een beetje met systeembanken, maar dan digitale-systeemleveranciers, als ik het even zo mag zeggen. Het is mijn primaire inzet – dat heb ik in de brief van gisteren ook aangegeven – om binnen de huidige kaders van de Wet beveiliging netwerk- en informatiesystemen de

mogelijkheden te maximaliseren, samen met collega-departementen, zodat we kunnen zien waar het tekortschiet. Daar kom ik dan spoedig op terug bij uw Kamer, zoals ik heb aangegeven. Het gaat dus om het maximaal benutten van de mogelijkheden op dit moment.

De heer **Middendorp** (VVD):
Dank voor het antwoord, maar ik ga toch één stap verder, want je kan je geld maar een keer uitgeven. Het woord «investeren» is ook al een paar keer gevallen. Als je besluit om niet met een A-team in te grijpen, en constateert dat er ook een zekere weerbaarheid vereist is, een verantwoordelijkheid bij – laten we in dit geval zeggen – kleine ondernemers ligt, dan is er nog een derde dat in ieder geval meegenomen zou moeten worden: de slagkracht van de overheid om online te handhaven. In de normale wereld treedt de overheid op als iemand gechanteerd wordt, en dat moet in de onlinewereld natuurlijk ook gebeuren. Dus als je besluit om niet in te grijpen, dan is er nog iets anders wat de overheid zou kunnen doen om bijvoorbeeld ondernemers online te helpen, namelijk het handhaven van bepaalde regels ten aanzien van phishing, ransomware en al dat soort dingen. Dat is een element dat ik eigenlijk een beetje mis. Want stel dat je 95 miljoen hebt, waar geef je het dan aan uit? Zet je teams op die potentieel ingrijpen, of geef je het uit aan betere handhaving online?

Minister **Grapperhaus**:
Dat zou natuurlijk ook een hoofdstukje moeten zijn in het onderzoek dat ik heb toegezegd. Ook daar moeten we naar gaan kijken. De verbondenheid van publiek en privaat, en van essentieel privaat met misschien minder essentieel privaat – maar wat weer een deel van een systeem of van wat dan ook levert – maakt dat het heel moeilijk is, in ieder geval voor mij in dit stadium, om inderdaad zonder diepgaand onderzoek vast te stellen waar welke maatregel door wie het beste zou moeten opgepakt. Maar in ieder geval denk ik dat er toch ook scherpte moet komen op een zeker overkoepeld toezicht en de mogelijkheden voor dat toezicht om op bepaalde momenten dringend aan te zetten tot actie. Ik zeg het liever wat voorzichtiger op deze manier dan dat ik het woord «doorzettingsmacht» gebruik, omdat dat woord bij allerlei spelers in het veld dan toch weer een soort onrust laat ontstaan. We moeten met elkaar gaan zoeken naar een methode die het mogelijk maakt om in ieder geval toch in bepaalde situaties iets opgelost te krijgen. Een dreigende ontwrichting moet wel voorkomen kunnen worden. Ik kom nog bij u terug op de vraag wat als het niet binnen de huidige wet, de Wet beveiliging netwerk- en informatiesystemen kan. Wat hebben we dan nog aan regelgeving nodig om dat in bepaalde noodsituaties mogelijk te maken? Ik wil ook echt voor de mensen die hier zijn of hiernaar kijken, duidelijk maken: we hebben het er niet over dat een systeem eens een keer dreigt vast te lopen waardoor de provider het via een Duits systeem moet laten lopen en de internetsnelheid van de Nederlandse burger omlaaggaat. Ik zei al dat ik er toch wel een zekere milde glimlach bij kan vertonen als veel Nederlanders dan protesteren. Maar het gaat om situaties waarbij bijvoorbeeld een onderdeel van onze vitale infrastructuur in zijn functioneren ernstig belemmerd wordt en waardoor het dagelijks leven ontwricht dreigt te worden. In dat soort situaties moeten we op niet al te lange termijn weten wat nog de ontbrekende schakels zijn die niet in de Wbni staan en die we als regelgeving nodig zouden hebben?

De heer **Middendorp** (VVD):
Een korte vervolgvraag. De vitale infrastructuur is een heel belangrijk onderwerp, maar laat ik het toch even terugbrengen naar die kleine ondernemers. Ik denk dat het misschien wel meer dan een hoofdstukje zou moeten zijn. Waarom? Ik zei het al: je kan je geld maar een keer uitgeven. Laat ik een voorbeeld geven. Als een ondernemer zijn

bedrijfspand niet goed beveiligt, dan kan je daar met toezicht maar ook met bewustwordingscampagnes en met het geven van informatie een heleboel aan doen. Maar tegelijk denkt die kleine ondernemer: de politie kan mij ook helpen beschermen tegen inbrekers. Die parallel is misschien wel relevant. Tegen ransomware kun je, simpel gezegd, twee dingen doen: toezicht houden en handhaven. Hoe kijkt de Minister daar nou tegen aan? Want dat is wel de basis voor de keuze: waar ga ik mijn geld aan uitgeven?

Minister **Grapperhaus**:
Mijn excuses voor het feit dat ik dan toch even in herhaling verval, maar ik vind het lastig om daar nu een uitspraak over te doen. Want gelet op dat digitale domein kunnen wij wel metaforen maken voor de fysieke wereld – u mag van mij ook zeggen: de analoge wereld, de analoog-fysieke of de fysiek-analoge wereld – maar die metaforen schieten op bepaalde punten gewoon tekort. Heel eerlijk gezegd vind ik het dus gevaarlijk om, voordat we een aantal dingen nader hebben uitgezocht, al aan te geven waar we nou precies de accenten op zouden moeten leggen. Maar ik ben het met u eens dat we die op enig moment wel goed moeten leggen. We moeten niet ons geld gaan inzetten op extra handhaving als achteraf blijkt dat we dat beter hadden kunnen inzetten op preventie, of zelfs al preventie bij de fabrikant. Daarmee dreig ik toch bijna weer een metafoor voor de werkelijkheid te maken, want we zien natuurlijk ook in het dagelijks leven dat in sommige gevallen preventie veel betere effecten oplevert dan repressie. Maar ik wijs erop dat mijn voorgangers – ere wie ere toekomt – de high-impact crime met speciale inzet en campagnes fors omlaag hebben gekregen. Daar zat een hele grote component preventie in, maar ook een grote component repressie in de vorm van lik op stuk. Dat zal dus verschillen per categorie.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Ik wil toch nog iets zeggen over het punt van de heer Middendorp. Hij zei: wij gaan mogelijk bij bedrijven een dringende toezichtactie opzetten, maar heeft u het zelf wel op orde? Dat moet in de komende tijd natuurlijk ook verder blijken. De organisaties binnen JenV acteren op dit moment tijdig op de kwetsbaarheidsmeldingen die door het NCSC aan het Security Operations Center, SOC, van het eigen ministerie worden gemeld. Die nemen ook de geadviseerde maatregelen. Maar die kwestie rondom de Pulsepatch, die nog niet door alle organisaties was geïnstalleerd, had te maken met het initiële beveiligingsadvies. Want het oplossingsproces van ICT-kwetsbaarheden in lijn overigens met bedrijfsvoeringsprocessen, adresseert de meest gevaarlijke kwetsbaarheden altijd als eerste. Maar goed, ik denk dat het snelle handelen van de JenV-onderdelen, die na het verhogen van het beveiligingsadvies binnen enkele dagen de updates hebben uitgevoerd, ervan getuigt dat men die gevaarlijkste kwetsbaarheden altijd als eerste adresseert. Ik heb de bijbehorende feiten en cijfers destijds bij die mondelinge vraag genoemd. Dan zie je dat dat loopt van april tot en met augustus. Na een waarschuwing «denk erom, twee organisaties moeten updaten» op 25 augustus van het NCSC aan het SOC van het eigen ministerie, is die update binnen 24 uur uitgevoerd. Nog even het volgende voor de duidelijkheid, anders begrijpen de mensen het niet meer: het NCSC valt onder mijn verantwoordelijkheid, maar opereert wel onafhankelijk ten opzichte van het functioneren van de digitale systemen van mijn eigen ministerie. Dat kan daar dus een eigen onafhankelijk oordeel op geven.
Voorzitter. Dan heb ik nog een paar vragen van de heer Van den Berge.

De **voorzitter**:
U heeft eerst nog een vraag van de heer Middendorp.

De heer **Middendorp** (VVD):
Dank aan de Minister voor de antwoorden. Ik wil nog even terugkomen op de vraag die aan het begin beantwoord werd, in ieder geval deels, over de samenwerking. Daar hebben we gisteren uitgebreid over gedebatteerd bij de begrotingsbehandeling BZK. De Minister verwees ook naar de verantwoordelijkheden die daar liggen. Mij valt op dat de enige die ik bij alle ministeries steeds maar tegenkom, hier zit. Dat is Kees Verhoeven. Dit is een gouden kans om hier wat over te kunnen zeggen, want op die verschillende ministeries is men heel druk aan het werk met de vraag: hoe kunnen we kennis delen? Dat betreft niet alleen samenwerken, zoals de Minister dat beschreef. Ik vroeg eigenlijk naar zo'n idee als een rijksinspectie digitalisering, die eigenlijk gewoon kijkt naar hoe het Ministerie van Financiën rijksbreed de financiën in onze overheidshuishouding coördineert. Bij het Ministerie van BZK wordt daar heel vaak over gesproken, maar is dat ook als een keer langsgekomen bij JenV? Ik zal niet helemaal uitleggen wat daarachter zit, maar heel veel van de samenwerkings- en aansturingsproblemen die hier aan de orde komen, zitten in dat voorstel.

Minister **Grapperhaus**:
Ik zit even na te denken hoe ik dat nou goed moet aanvliegen. Ik heb het systeem zoals het nu in elkaar steekt, uiteengezet. Ik heb duidelijk toegegeven dat de ervaringen in het proces bij de diverse toezichthouders nog moeten komen. Je zult daar dus een aantal dingen moeten ontwikkelen. Daar neemt mijn inspectie het voortouw in en het coördineert dit ook, zodat we daar in ieder geval in verder komen. Dat is één belangrijk ding. Verder zal de samenwerking tussen departementen erop gericht moeten zijn om inderdaad kennis te delen met elkaar. Via die voortrekkende rol van de Inspectie JenV en die aanjagende en toezichthoudende rol van het NCSC zul je verder moeten komen in je kennis en je aanpak. Dat lijkt me heel duidelijk. Vervolgens heb ik gezegd dat we, als we alle instrumenten van de huidige wet hebben uitgenut, met elkaar moeten bekijken of er toch meer mogelijkheden via regelgeving moeten komen. Die zullen er dan ook op gericht moeten zijn om dit te optimaliseren. Hoe dat er op dit moment uitziet? Zover zijn we nog niet, denk ik, juist omdat we de Wbni ook bedoeld hadden om alles zo veel mogelijk te regelen.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Ik kom bij de vragen van de heer Van den Berge. In de tweede termijn zal ik terugkomen op het punt van de meldkamer. De heer Van den Berge zei dat de incidenten vaak het resultaat zijn van laksheid; ik geloof dat hij dat woord gebruikte. Hoe moet je dat nou gaan aanpakken? Ik heb dat net al ietwat anders gezegd, maar het gaat om de gebruikmaking van interventiemogelijkheden en om die zo veel mogelijk te maximaliseren. Wat mij betreft kan het NCSC onder de huidige regelgeving al richting de sectorale toezichthouders escaleren als beveiligingsadviezen, zoals bij Pulse, niet worden opgevolgd. Ik heb dat net al genoemd. Laten we onze eigen tekortkomingen bij JenV als voorbeeld nemen. Daar zag je dat het op 25 augustus nog niet op orde was. Toen is het eigen Security Operations Center van het ministerie aangesproken door het NCSC: dit moet nu in orde komen; er zijn er nog twee die er niet aan voldoen. Dat is binnen een dag gebeurd. Dat is misschien een ideale wereld of zo zou het dan moeten gaan, maar het belangrijkste daarbij is dat het NCSC een centrale informatiepositie heeft. Ik heb eerder gezegd dat zij, ook door de

sectorspecifieke kennis die ze natuurlijk moeten hebben, kunnen zien waar mogelijk kwetsbaarheden binnen de vitale infrastructuur ontstaan. Ik ben ervan overtuigd dat het intensiveren van de samenwerking tussen toezichthouders aan de ene kant en het uiteindelijk ook versterken van de toezichthouders en het NSCS aan de andere kant, ingrijpen sneller mogelijk maakt. Nogmaals, u hoort mij nu voorlopig even de term «dringend aanspreken» gebruiken in plaats van het woord «doorzettingsmacht». Ik zei het al: dat woord veroorzaakt hier en daar wat onrust en ik wil eerst met uw Kamer in gesprek gaan om te bedenken wat er volgens ons nog ontbreekt. Is dat doorzettingsmacht in een bepaalde dreigende ontwrichtingssituatie? Of is het al voldoende om te zeggen: er moet nu een dringende aanspreekmogelijkheid zijn, zoals naming-and-shaming en dat soort dingen?
Voorzitter. Dan de kwestie van de leverancier van Russische antivirussoftware. Is er nou een relatie tussen die discussie en de discussie over 5G? In mijn brief over de Russische antivirussoftware en de leverancier daarvan heeft u kunnen lezen dat het uitgangspunt is dat wordt gekeken of er sprake is van een bedrijf dat zijn stevige basis heeft in een land dat wordt gekwalificeerd als een statelijke actor. Of een land wordt gekwalificeerd als een statelijke actor, wordt bepaald door onze inlichtingendiensten, de MIVD en de AIVD. Het tweede punt is: is er sprake van software of andere digitale technologie die zeer ver in onze systemen kan komen, daarvoor een potentiële bedreiging kan vormen en de boel in negatieve zin kan beïnvloeden? Als je die twee hordes hebt genomen en met «ja» hebt beantwoord, dan is de derde: in hoeverre kunnen die risico's goed gemitigeerd of uitgebannen worden en zo geminimaliseerd worden? En dan ten slotte: dat wordt altijd case-by-case, van geval tot geval, beoordeeld. Ik vind dat dat in het kader van de proportionaliteitstoets ook moet gebeuren, want je kunt niet zomaar zeggen: nou, men komt uit land X, het is een statelijke actor, het gaat heel ver de systemen in, dat is helder, en we hebben geen vertrouwen in de risicomaatregelen. Nee, je moet dat grondig doen en steeds per geval opnieuw de beoordeling maken, zonder in algemeenheden te vervallen.

De heer **Van den Berge** (GroenLinks):
Ik waardeer dit antwoord van de Minister over de conceptuele aanpak, maar daar zit eigenlijk precies mijn vraag. Want de brief van de Minister over die Russische leverancier, Kasperskay – ik hoor net dat ik «Kasperskie» moet zeggen; ik weet trouwens niet of dat Cybersecurity Woordenboek ook fonetisch is? – lees ik toch alsof andere leveranciers uit Rusland ook niet in aanmerking zouden komen om diensten aan de overheid te leveren. Maar dat lees ik dan dus niet goed. Zo lees ik die brief wel, met de drie overwegingen van de Minister om deze specifieke fabrikant uit te faseren. Het gaat heel erg over de invloed die Russische overheidsdiensten hebben, et cetera, et cetera. Mijn vraag zit hem inderdaad precies daarin: wanneer kan een landengerichte aanpak wel en wanneer kiest de Minister voor een case-by-casebasis, zoals hij in de discussie over Huawei en 5G steeds zegt? Precies daar zit mijn punt.

Minister **Grapperhaus**:
Het is niet zo dat het meteen buut vrij is voor iedere partij uit een land dat een offensief cyberprogramma heeft, want dat verstaan we eigenlijk onder een statelijke actor. Nee, daarvoor is nou juist die cumulatie- of escalatieladder; hoe je die noemt, zullen we nooit weten, en dat staat ook niet in dat woordenboekje. Daarvoor pak je drie trappen. Eerst kijk je of het een land met een offensief cyberprogramma is. Als dat het geval is, zeg je... Ik zou bijna nog vergeten: heeft dat land ook wetgeving die bedrijven dwingt om mee te werken? Dat is overigens vaak congruent of komt tegelijk voor, maar het moet ook een land zijn met niet alleen een offensief cyberprogramma tegen Nederland, maar ook wetgeving die

bedrijven dwingt om mee te werken als men dat wil. Dan komt de volgende: gaat het product heel diep in de systemen? Als allerlaatste ga je bekijken: oké, maar zijn er toch nog adequate maatregelen te treffen op het gebied van beveiliging, zodat je ook in deze situatie toch voldoende cybersecurity hebt?
In het geval van deze Russische leverancier hebben de diensten informatie aangeleverd, en heeft de NCTV een afweging gemaakt en gezegd: wij denken dat dat toch echt niet door de test heen komt. Maar nogmaals: dat gebeurt dus steeds case-by-case.

De heer **Van den Berge** (GroenLinks):
Ik denk dat we er vandaag niet uitkomen. Maar om heel eerlijk te zijn, baart het antwoord mij wel zorgen. Als ik het goed hoor, zegt de Minister eigenlijk: als de software van andere leveranciers uit Rusland er net iets anders uitziet, dan komen ze misschien wel door de toets heen. Hij zegt dat het case-by-case gebeurt en dat er aan allerlei criteria getoetst moet worden. Dat baart me toch wel zorgen, want wetgeving evolueert en technieken evolueren. Als we gewoon weten dat het gaat om overheden met een vrij agressief beleid waar het gaat om bijvoorbeeld cyberspionage en het opvragen van data, dan denk ik dat we heel terughoudend zouden moeten zijn met het inkopen van software uit dergelijke landen.

Minister **Grapperhaus**:
Laten we even een concreet voorbeeld nemen. Kijk, stel dat er een leverancier is uit een land dat wordt gekwalificeerd als een land dat een tegen Nederland gericht offensief cyberprogramma heeft. Dat maken onze inlichtingendiensten uit; laat dat duidelijk zijn. Dat land heeft in zijn wetgeving ook de mogelijkheid dat de overheid tegen een dergelijk bedrijf kan zeggen: jullie moeten nu even doen wat wij willen; je moet dit chipje in je apparaten zetten. Een manipulatiechipje dus vanuit de overheid. Dan kan het nog steeds gaan om software die helemaal niet diep in de systemen gaat, maar die misschien – ik noem maar wat – het geluid van de waarschuwingsbel in ons parlement reguleert op hard en zacht. Dan kun je zeggen dat dat volstrekt niet relevant is en dat het software betreft die volstrekt niet onze systemen in gaat. Dan zou die dus nog steeds geleverd kunnen worden. Daarbij speelt dan overigens nog steeds de kwestie van de eventuele risico's die gepaard gaan met die software. Zijn die er en, zo ja, kun je die mitigeren? Ik denk dus dat daar voldoende terechte barrières in zitten, die wel recht doen aan het proportionaliteitsbeginsel.

De heer **Verhoeven** (D66):
Ik merk dat ik er anders in zit dan GroenLinks. Ik herinner me wel eerdere debatten over dit onderwerp en ik herinner me ook wat recente berichten uit de media. Ik herinner me ook dat ik bij een debat ben geweest waar de directeur van Kaspersky bij aanwezig was. Ik heb toch nog wel een aantal vragen nu dit zo naar voren komt. De eerste vraag is: wat heeft Nederland nou draaien van Kaspersky? Want er wordt wel gezegd dat wij als overheid die leverancier gaan bannen, maar ik heb ook vernomen dat helemaal niet bekend is welke ministeries nu eigenlijk antivirussoftware van Kaspersky hebben draaien. Dat vond ik een opvallend gegeven, waar ik de Minister toch nog eens naar wil vragen. Ik hoor nu trouwens de bel van de plenaire zaal gaan. Die doet het dus nog, maar de Minister wordt er niet door gered.
Het tweede is dat Kaspersky heel graag de zorgen wil wegnemen die er zijn. Ze hebben allerlei pogingen gedaan en heel veel dingen laten zien, zo heb ik vernomen, om te bewijzen dat ze op dat case-by-caseniveau en dat technische niveau juist niet bewust mogelijkheden bieden om hun software te laten gebruiken voor afluisteren of andere inmengingsdoel-

einden van de Russische overheid. Ik zou dus toch van de Minister willen weten wat hij van deze twee punten vindt.

Minister **Grapperhaus**:
Laat ik beginnen met te zeggen dat dit een heel zorgvuldige afweging is. Er wordt periodiek gekeken welke bedrijven wel of niet aan bepaalde eisen voldoen. En dan zijn er natuurlijk ook nog de ontwikkelingen in de technologie die hierop gaandeweg van invloed kunnen zijn. Als de heer Verhoeven mij vraagt om een gedetailleerd overzicht te geven van waar die antivirussoftware nou precies in zat, moet ik hem dat antwoord nu even schuldig blijven, want dat gedetailleerde overzicht kan ik op dit moment niet geven. Ik kan wel zeggen dat het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties op dit moment bezig is met de uitfasering, en dat de Kamer eind dit jaar hoort hoe het daar precies mee is gesteld. Maar tegen beide Kamerleden zeg ik toch even, hoewel zij het onderling kennelijk niet helemaal eens zijn, dat dit juist een proces is van zorgvuldige afweging naar twee kanten toe. Dat is aan de ene kant naar het beginsel van cybersecurity, en aan de andere kant ook naar het beginsel dat het natuurlijk wel een zorgvuldige afweging moet zijn geweest als je op een bepaald moment in het licht van de cybersecurity zegt dat het niet meer verstandig is om met de diensten of producten van een bepaalde partij te werken. Dat moet ook een zorgvuldige afweging blijven, ook weer gezien latere technologische ontwikkelingen.

De heer **Verhoeven** (D66):
Oké. Ik heb als Kamerlid een paar instrumenten. En al die instrumenten zijn niet voldoende om te achterhalen of er naast de drie criteria in de cumulatieladder van de Minister nog iets anders aan de hand is waardoor hij inderdaad op zorgvuldige en proportionele wijze heeft besloten om de antivirussoftware van Kaspersky niet meer te gebruiken. Want ik ken wel die drie criteria – die zijn gewoon openbaar in een brief gezet – maar ik ken niet het NCTV-onderzoek waar de Minister naar verwijst, met daarin de case-by-casevoorbeelden, de technische aanwijzingen of de zaken die voldoende twijfel genereren om dit besluit zorgvuldig te kunnen nemen. Ik zal de Minister ook niet vragen om die openbaar te maken, want ik weet dat dat niet kan. Kijk, ik ben er helemaal geen voorstander van dat allerlei Chinese en Russische bedrijven hier diep in onze systemen zitten. Ik denk niet: nou, daar wordt het lekker veilig van. Dus voor de onderbuik van een Kamerlid voelt het prima om dit zo te doen. Maar dit gaat om de manier waarop je omgaat met een bedrijf dat misschien verdacht is op basis van drie algemene criteria. Dan vind ik het toch lastig om niet te kunnen weten wat er echt aan de hand is. Ik vraag dat niet aan de Minister, maar ik vraag hem wel om te reageren op dit probleem dat ik als Kamerlid heb. Hoe kunnen we hier in de toekomst besluitvorming over hebben? Ik kan de Minister namelijk op deze manier niet controleren, en de heer Van den Berge ook niet. En dan heb ik het nog niet eens over de twee kanonnen naast mij, Middendorp en Van Dam.

Minister **Grapperhaus**:
Ik moet toch even afstand nemen van deze dichotomie van vandaag in de samenstelling van uw commissie, want ik acht alle vier de leden in menig opzicht kanonnen.

De heer **Van Dam** (CDA):
Case-by-case.

Minister **Grapperhaus**:
Ja, ik heb het dan over Kees, maar ook over de andere drie cases.

De **voorzitter**:

Fijn. Hartelijk dank.

Minister **Grapperhaus**:
Voorzitter. Ik keer even terug naar het punt van de heer Verhoeven, dat ik begrijp. Dat is natuurlijk niet meer te volgen, zeker niet voor de mensen die dit proberen te volgen. De heer Verhoeven zegt: Minister, ik snap eigenlijk wel dat u niet meer inzage kan geven, maar ik zit daar wel mee, omdat ik daardoor onvoldoende inzage heb. Ik zeg eigenlijk hetzelfde. Ik snap heel goed dat u vindt dat u mij zo niet helemaal goed kunt controleren, maar aan de andere kant kan ik u niet meer inzage geven. Het enige wat ik kan doen om te proberen om die impasse te doorbreken, is erop wijzen – dat zit ook in de brief over Kaspersky – dat we die criteria heel duidelijk benoemen. Uit die brief kunt u afleiden hoe wij de trap opbouwen.
Ik heb in de brief, in publicaties nadien en ook in reactie op Kamervragen en dergelijke heel duidelijk gezegd dat wij het land van de thuisbasis van Kaspersky zien als een ten opzichte van Nederland cyberoffensief land. Ik heb ook verantwoord dat sprake is van software die diep in die systemen doordringt. Ik probeer toch even om te kijken of we uit die impasse kunnen komen. Het eerste punt is natuurlijk gebaseerd op kennis van onze inlichtingendienst; daar kan ik inderdaad niet veel meer over zeggen. Het tweede punt is gebaseerd op het volgende. Als de Tweede Kamer zou zeggen dat ze getoetst wil hebben of die antivirussoftware van Kaspersky echt zo diep in die systemen zit, kunt u, als u dat zou willen, natuurlijk nog een andere deskundige vragen om een opvatting. Maar laten we voor de sake of purity, voor de zuiverheid en het vertrouwen in elkaar ervan uitgaan dat dat ook echt klopt.
Dan komt u op het derde punt uit. U vraagt: is dit dan vervolgens software waarvan we zeggen dat daar onvoldoende risicomitigerende maatregelen tegen te nemen zijn? Daar kan ik tot op zekere hoogte informatie over geven, door te zeggen: zo diep gaat het in die systemen en dit zijn de risico's die zich voordoen. Maar op een gegeven moment schiet ik tekort in uitleg, omdat ik niet aan uw Kamer kan gaan uitleggen wat er nu precies aan vertrouwelijke of geheime maatregelen getroffen zouden kunnen worden. Dan kom ik namelijk op een hellend vlak terecht. Maar ik meen wel dat het blootleggen van die criteria het voor uw Kamer mogelijk zou moeten maken om tot op zeer grote hoogte nog te kunnen controleren hoe het werkt.
Voorzitter. Ik kom nog aan twee vragen van de heer Van den Berge toe. Dan ga ik nog even terug naar de heer Verhoeven over dat inspectierapport.

De **voorzitter**:
Een ogenblik, want ik moet de vergadering helaas verlaten, zoals aangekondigd. Ik heb de heer Van Dam bereid gevonden om het voorzitterschap over te nemen. Ik wens u allemaal nog een mooie middag.

Voorzitter: Van Dam

Minister **Grapperhaus**:
Dank, voorzitter, voor uw voorzitten.
Dan ga ik nog heel kort in op twee vragen van de heer Van den Berge over ISIDOOR. De laatste keer was in 2017, en in de zomer van 2020 zal de volgende ISIDOOR-stresstest plaatsvinden.
Dan kom ik op dat oefenen en testen. Dat gaat in die grootschalige cyberoefening ISIDOOR gebeuren. Overigens is het zeker mijn voornemen om dat structureel te doen. Ik zal u via de al aangekondigde uitwerking van het versterkingsprogramma informeren over verdere plannen over zo'n oefen- en testprogramma, naast een aparte van ISIDOOR.

Ten slotte, voorzitter, over dat inspectierapport voor de behandeling van de Wijzigingswet meldkamers. Dat gaan we qua tijd dus niet redden, maar ik zal nog in een brief aan uw Kamer uiteenzetten dat dat niet zou behoeven te raken aan de behandeling van de Wijzigingswet meldkamers. Dat wil ik dus bij dezen toegezegd hebben.
Voorzitter, ik heb dan alle vragen beantwoord.

De heer **Van den Berge** (GroenLinks):
Ik heb een korte, verhelderende vraag over de stresstesten en over ISIDOOR. De Minister van plan te zijn dat structureel te maken. Bedoelt hij met «structureel» dat we het vaker gaan doen? Want 2017–2020: dat is toch een gat van maximaal drie jaar. Misschien iets korter, maar...

Minister **Grapperhaus**:
Ja, bijna net zoals bij de Olympische Spelen. Maar ik ben het helemaal met u eens dat we ook gaan kijken hoe we vaker een misschien kleinere, meer gerichte stresstest met elkaar kunnen gaan doen. Daar kom ik op terug in de uitwerking van het versterkingsprogramma.

De **voorzitter**:
Ik kijk even of er op voorhand nog onbeantwoorde vragen bij de leden leven. Ik moet eerlijk zeggen dat ik er wel eentje heb, namelijk over de toekomst van het Digital Trust Center. Of heb ik dat antwoord gemist?

Minister **Grapperhaus**:
Voorzitter, u heeft in zoverre gelijk, althans, de heer Van Dam heeft in zoverre gelijk, dat ik wilde zeggen – dat heb ik verzuimd – dat ik aan de Staatssecretaris van EZK zal vragen om nog met een brief hierover te komen. De heer Van Dam heeft een ambitie naar voren gebracht, en het is iets dat op het terrein van deze Staatssecretaris ligt. Eind van dit jaar wordt dat Digital Trust Center overigens geëvalueerd. In ieder geval komt er in januari 2020 een brief van EZK, maar ik zal dus de wens overbrengen van uw Kamer dat daarin de ambities duidelijk worden geformuleerd, voor zover dat al niet het plan was.

De **voorzitter**:
Goed. Dan dankt de heer Van Dam via de voorzitter de Minister voor dit antwoord. We gaan nu naar de tweede termijn. We hebben een minuut de tijd per spreker. Daar houd ik u aan.

De heer **Verhoeven** (D66):
Dat kunt u zeker doen, meneer voorzitter. Ik zou de heer Van Dam daar ook aan houden, als ik u was!
Dank aan de Minister voor de beantwoording van de vragen, in het bijzonder het laatste stuk, maar ook wel de opmerkingen die zijn gemaakt over alles wat te maken heeft met het NCSC. Ik denk dat die organisatie nóg meer kan excelleren als ze de juiste bevoegdheden en mogelijkheden heeft binnen het speelveld met al die spelers die zich ook uitlaten over en actief bezig zijn op het gebied van cybersecurity.
Ik dank de Minister ook voor zijn ruimhartige toezegging om te gaan onderzoeken wat er nodig is aan investeringen om de digitale veiligheid in Nederland veilig te stellen. Ik zou hem wel willen vragen hoe hij dat gaat doen. Wordt dat echt een onafhankelijk onderzoek door een organisatie die dit gewoon in beeld kan brengen? Het is natuurlijk interessant om dat getal op een of andere objectieve manier te hebben. Dat is ook van belang met het oog op de toekomst.
Verder zal ik zelf ook nog eens even nagaan of ik het eens ben met de Minister dat 112-back-up, het onderzoek van de inspectie en de meldkamerwet inderdaad los van elkaar staan. Ik twijfel daaraan, maar ben nu

geneigd om maar genoegen te nemen met het antwoord dat de Minister heef gegeven. Maar dat is dan wel voor dit moment.

De **voorzitter**:
Dank u wel, meneer Verhoeven. Dan nu de heer Middendorp.

De heer **Middendorp** (VVD):
Dank, voorzitter. Ook dank aan de Minister voor de antwoorden en het debat. Zeker ook dank voor het boekje; ik zal het ook bij andere ministeries kunnen gebruiken, verwacht ik, dus heel veel dank.
Dank ook voor de net toegezegde brief over dat Digital Trust Center. Toen ik de getallen, zestien mensen op 1,3 miljoen bedrijven, eenmaal had opgezocht, dacht ik: nou, dit ga ik toch wel even naar voren brengen. Maar dit is ook een opzetje geweest naar de discussie over de balans tussen het aanpakken van digitaal tuig – ik zeg het maar even in analoge-wereldtermen – en het toezicht en de informatieverstrekking aan de voorkant. Aan de ene kant gaat het dan natuurlijk over het besteden van geld en het maken van keuzes. Dat doen wij hier de hele dag. Maar het geeft ook heel duidelijk aan dat er, in ieder geval mijns inziens, een soort schijnzekerheid in de digitale wereld is, als zou je van alles van tevoren kunnen regelen met toezicht en het geven van informatie. Uiteindelijk echter, denk ik, gaat het ook gewoon om handhaven en het aanpakken van digitaal tuig, zoals ik al zei. Maar zoals de Minister al heeft aangegeven, is dit iets wat nog duidelijk vervolgd zal worden.
Dank, voorzitter.

De **voorzitter**:
Dan de heer Van den Berge.

De heer **Van den Berge** (GroenLinks):
Voorzitter. Ik dank de Minister voor zijn uitgebreide beantwoording en de toezeggingen. Ik vind het positief dat er vaker stresstesten zullen worden gedaan. We komen er op een later moment nog over te spreken hoe dat er concreet uit gaat zien, maar dat is positief. Een van mijn vragen in dit algemeen overleg was namelijk hoe we dingen concreter kunnen maken. Het is goed dat we meer willen gaan oefenen, meer ervaring op willen doen, maar hoe gaan we dat concreet doen? Daar hebben we vandaag echt wel vooruitgang in geboekt. Dat is positief.
Over Kaspersky en Huawei hebben we voor nu genoeg gewisseld, want daar komen we vandaag toch niet verder mee. Daar komen we later nog wel over te spreken. Wat mij wel heel duidelijk werd, ook door het interruptiedebat van collega Verhoeven met de Minister, is dat er een zeker ongemak zit in de beperkte mate waarin we de informatie over risico's en incidenten kunnen delen. Dat begrijp ik, zeker daar waar de inlichtingendiensten betrokken zijn en waar de staatsveiligheid een rol speelt, maar tegelijk hebben we die kennis natuurlijk wel nodig, zowel voor ons als Kamerleden om onze controlerende taak te kunnen vervullen alsook voor private partijen om een goede risico-inschatting van specifieke leveranciers te maken. Ik heb kennisdeling in mijn eerste termijn ook kort genoemd. De schrijver Modderkolk heeft het er in zijn boek ook over dat daar een lastigheid in zit, omdat we bij cybersecurity-incidenten vaak minder kennis tot ons kunnen nemen dan bij andere incidenten. Dat is deels begrijpelijk, maar daar zit wel een zeker dilemma. Misschien kan de Minister daar nog kort op reflecteren.
Bedankt.

De **voorzitter**:
Dank u wel, meneer Van den Berge.
Ik heb zelf in mijn tweede termijn namens de CDA-fractie nog twee vragen. In de eerste plaats heb ik nog geen volledig antwoord gekregen

op de vraag hoe informatie terugloopt vanaf het NCSC naar die vitale sectoren. Je moet toch een situatie krijgen waarin men niet alleen hoeft te leveren maar ook iets terugkrijgt, en misschien ook wel redelijk sectoraal. Misschien dat daar nog een antwoord op kan komen.
Mijn tweede punt betreft het oefenen. Ik vind het heel mooi dat er een stresstest komt, maar volgens mij is dat niet het enige wat nodig is. Zoals je in de werkelijkheid oefent met bijvoorbeeld een epidemie die eraan komt of een stormvloed die ons land overspoelt, moet er volgens mij ook geoefend worden met een bepaalde activiteit die zich wellicht voordoet. Dat vind ik toch net wat anders dan een stresstest; dat vind ik wat algemener. Misschien kan de Minister nog iets uitdrukkelijker de vraag beantwoorden of tijdens de nationale crisisoefeningen ook dit soort dingen geoefend worden. Dat zijn mijn opmerkingen.
Ik weet niet of de Minister meteen kan antwoorden. Door op te staan doet hij vermoeden dat hij dat inderdaad kan. Dat is heel fijn.

Minister **Grapperhaus**:
Ja, voorzitter. De heer Verhoeven vroeg naar dat onderzoek. Dat moet grondig zijn. We moeten echt even kijken wat de juiste partij is. Ik ben heel voorzichtig met te zeggen dat de Wetenschappelijke Raad voor het Regeringsbeleid daar geschikt voor zou zijn, want dan hebben we ook weer te maken met de net door u beschreven gemiddelde reactietijd. Dat ligt niet aan de WRR, maar dat ligt aan het feit dat er veel departementen bij betrokken zijn. Maar ik denk wel dat een partij van een dergelijke standing dit moet gaan bekijken.

De **voorzitter**:
De heer Verhoeven heeft hier een vraag over.

De heer **Verhoeven** (D66):
Ja, dat heb je in een debat weleens, dat er vragen worden gesteld. Dat de Minister de WRR noemt, vind ik een aanwijzing dat de Minister dit serieus neemt. Daar ben ik blij mee. Van mij hoeft het dat dus niet te zijn en kan het alle kanten op. Ik zou het prettig vinden als de Minister een brief aan de Kamer zou willen sturen waarin hij kaders schetst en een en ander samenvat. Dat wordt overigens gedaan, want dat is een toezegging die de Minister heeft gedaan, dus die wordt dan schriftelijk genoteerd. Maar ik zou dus graag een brief willen waarin de Minister kort uiteenzet hoe hij dit voor zich ziet, omdat ik hier echt waarde aan hecht. Ik vind het echt een belangrijke stap, ook voor de toekomst. Ik ben dus ook wel heel blij met deze toezegging; vandaar nog deze aanvulling. Ik zal vanaf nu ook mijn mond houden.

Minister **Grapperhaus**:
Die brief is bij dezen toegezegd. Wat dat betreft vind ik het zeer plezierig dat we veel verder komen in dit overleg. Dat lijkt me dus heel erg goed. Ik zeg daar meteen achteraan dat we in de uitwerking van het versterkingsprogramma ten aanzien van de oefeningen en de tests niet alleen zullen komen met voornemens tot stresstests maar juist ook die systeemtests en andere tests. Als die uitwerking er is, moeten we dus goed met elkaar bespreken of u dat geruststelt en tot tevredenheid stemt. Het is in ieder geval de bedoeling om dit verder te laten gaan dan alleen de stresstests.

De **voorzitter**:
Ik heb even een vraag aan de Minister. U heeft al een aantal dingen toegezegd. Hoe moeten we dat zien? Komt er één brief waarin meerdere dingen staan? Komt die brief op 20 juni? Ik heb begrepen dat dit voor u een belangrijke datum is. Hoe moet ik dat zien?

Minister **Grapperhaus**:

Dat is de langste dag. Eigenlijk is dat op 21 juni natuurlijk, maar in het kader van de seizoenswisselingen kan dat soms net iets anders vallen; daar moeten we het later nog maar eens over hebben. We moeten zo even de toezeggingen op een rijtje zetten en kijken welke bij elkaar in één brief zouden kunnen. Het gaat mij in ieder geval om het volgende. Ik sprak net al mijn dank uit voor het feit dat u mij vraagt een aantal punten te verduidelijken. Dat doe ik dus graag. Dan kan ik dat ook met andere departementen delen en zeggen: we gaan nu op dit punt ook echt met een volgende fase en een verduidelijking komen. Als u het goed vindt, kunnen we straks even kijken wat er gecombineerd kan worden in brieven.
Met het kennisdelen richting het NCSC ben ik het helemaal eens, maar daar heb ik al het nodige over gezegd. Dat wordt ook alleen maar aangemoedigd. We hebben de Information Sharing and Analysis Centers. Verder is er ook sprake van de vrijwillige responsible vulnerability disclosure-melding; nogmaals excuus voor de niet-Nederlandse taal. We gaan natuurlijk met elkaar bekijken of dat voldoende is.
Dan had ik nog een vraag van de heer Van der Berge. Er is natuurlijk een andere commissie van uw Kamer die wel kan toetsen op het punt van bepaalde onderliggende informatie van inlichtingendiensten. Ik vermoed een beetje dat de heer Verhoeven aan de ene kant enigszins zijn impasse formuleerde, maar aan de andere kant zei hij dat hij dat vertrouwen wel wil geven omdat op een ander punt in de Kamer de toets van die informatie zonder meer aan de orde komt. Dat komt daar natuurlijk aan de orde, in de wetenschap dat het hier in het openbaar besproken is.
Dan heb ik volgens mij alle vragen beantwoord, voorzitter. We moeten dus alleen nog kijken naar hoe die diverse brieven zich qua timing tot elkaar verhouden.

De **voorzitter**:
Ja, ik denk dat we daarmee komen aan dat deel van de wedstrijd. Ik vraag de collega's uitdrukkelijk om even mee te luisteren, omdat ik niet de hele vergadering heb voorgezeten. Wij hebben twee toezeggingen genoteerd.
– In de eerste plaats zegt de Minister toe een onderzoek te gaan doen naar de benodigde investeringen bij de overheid op het gebied van cybersecurity. Een brief over de aanpak van dit onderwerp wordt aan de Kamer toegestuurd.

Ik denk dat in die brief ook aan de orde komt wat de gedachte is over wie dat onderzoek zou kunnen gaan uitvoeren. Ik kijk even naar de Minister voor een reactie hierop, maar ik zal eerst de tweede toezegging noemen.
– De Minister zegt toe de Kamer per brief te informeren over de raakvlakken van de Wijzigingswet meldkamers met de vitale infrastructuur, vóór de behandeling van deze wet.

Ik denk dat die laatste toezegging op kortere termijn geldt.

Minister **Grapperhaus**:
Ja, het moge duidelijk zijn dat, als die wetsbehandeling in december plaatsvindt – ik gooi het balletje voorzichtig op – we uiterlijk eind november aan uw Kamer moeten uitleggen waarom dat niet zou moeten uitmaken voor die wetsbehandeling. Dan heeft u nog ruim de tijd om daar een standpunt over in te nemen.

De **voorzitter**:
Wat de eerste toezegging over het onderzoek betreft, heb ik u ook nog gehoord over een toezegging om iets over het oefenen te melden aan de Kamer.

Minister **Grapperhaus**:
Ja, maar dat komt bij de uitwerking van de versterkingsplannen. Ik kijk even naar rechts: Q1 2020? Dat is in het eerste kwartaal in 2020.

De **voorzitter**:
Q?

Minister **Grapperhaus**:
Ja, Q.

De **voorzitter**:
Ik ben uit de tijd van Q & Q, dus vandaar dat ik er even naar vraag.

Minister **Grapperhaus**:
Ik durf het bijna niet te zeggen – ik ben nog iets ouder – maar ik ben uit de tijd van OQ.

De **voorzitter**:
OQ?

Minister **Grapperhaus**:
OQ. Dat was een stichting die zich richtte op veiligheid in het dagelijks leven. Werkelijk waar. Het is iets uit de jaren zestig. Dus ik neem niemand iets kwalijk als men niet weet waarover ik het heb.

De **voorzitter**:
Ik zeg u toe dat ik het allemaal op ga zoeken na de vergadering. Maar wanneer kunnen wij überhaupt een vervolgbrief verwachten? Misschien dat het daarin zou kunnen worden meegenomen om enige efficiëntie te bieden?

Minister **Grapperhaus**:
U was iets later, dus het kan zijn dat u het gemist hebt. Ik zet het even uit mijn hoofd op een rij en kijk ook even naar de griffier.
Ik heb aangegeven dat het nationaal crisisplan ICT eind dit jaar komt. Dan hebben we een maand eerder, eind november, dus al een briefje gehad over waarom dat wetsvoorstel niet in de weg staat aan het feit dat er pas later wordt ingegaan op de 112-crisis. Verder heb ik gezegd dat in Q1 een beleidsreactie komt op het WRR-rapport over de digitale-ontwrichtingsgevaren. Met die reactie komt een uitgewerkt voorstel voor het onderzoek en degene die dat zou moeten doen; daarover heeft de heer Verhoeven het gehad. Die twee zijn duidelijk aan elkaar gelinkt. Dan hebben we ieder jaar de voortgangsrapportage naar aanleiding van het Cybersecuritybeeld Nederland en die komt uiterlijk 20 juni, namelijk in het voorjaar. Daarin vindt ook de uitwerking plaats van het versterkingsprogramma en daarmee ook van wat er meer zou moeten gaan gebeuren op het gebied van oefeningen behalve alleen die stresstests. Dan komt ISIDOOR III in de zomer van 2020. Dan wordt een reeks oefeningen gedaan. Ik kijk even naar u en naar uw griffier, maar hiermee heb ik het volgens mij opgesomd.

De **voorzitter**:
We gaan het ook allemaal naluisteren op de band. Nog twee dingen dan. Wanneer komt de brief over de benodigde investeringen in het onderzoek waarnaar de heer Verhoeven heeft gevraagd?

Minister **Grapperhaus**:
Die komt dus in de beleidsreactie op het WWR-rapport in het eerste kwartaal van 2020.

De **voorzitter**:
Oké. En u zou nog contact opnemen met uw collega van Economische Zaken over het Digital Trust Center. Dat noteer ik ook maar even als een toezegging, althans een die doorgaat naar het erf van uw collega.

Minister **Grapperhaus**:
Die toezegging zal ik de komende weken zodanig nakomen dat zij in haar evaluatie van januari 2020 haar bevindingen in het kader van het Digital Trust Center kan meenemen.

De **voorzitter**:
Goed. Dan kijk ik nog even naar rechts om te zien of alles daarmee gedekt is. Ik zie knikkende mannenhoofden, dus dat moet goed gaan. Dan denk ik dat we daarmee tot een afronding zijn gekomen van dit AO. Wellicht was het aantal deelnemers niet hoog, maar daarmee was de kwaliteit en het soortelijk gewicht van de bijdragen van een ongekend hoog niveau, waarvoor ik de collega's dank.

De heer **Verhoeven** (D66):
Dat viel mij ook op!

De **voorzitter**:
Ik dank de Minister voor zijn uitgebreide beantwoording. Ik dank ook alle ambtenaren hier en verder weg die daaraan hebben bijgedragen. Ik dank de mensen op de publieke tribune en de mensen thuis voor hun interesse. Dank u wel.

Sluiting 17.19 uur.