Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

28 684 Naar een veiliger samenleving

Nr. 645

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 8 januari 2021

De vaste commissie voor Justitie en Veiligheid, de vaste commissie voor Binnenlandse Zaken en de vaste commissie voor Economische Zaken en Klimaat hebben op 9 december 2020 overleg gevoerd met de heer Grapperhaus, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 23 januari 2020 inzake overzicht op hoofdlijnen Citrix-kwetsbaarheden (Kamerstuk 26 643, nr. 660);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 22 april 2020 inzake reactie op verzoek commissie om informatie over berichtgeving dat Universiteit Maastricht losgeld heeft betaald (Kamerstuk 26 643, nr. 678);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 20 mei 2020 inzake internetcriminaliteit (Kamerstuk 28 684, nr. 621);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 25 mei 2020 inzake antwoorden op vragen commissie over onder andere overzicht op hoofdlijnen Citrix-kwetsbaarheden (Kamerstuk 26 643, nr. 685);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 29 juni 2020 inzake cybersecuritybeeld Nederland 2020 (CSBN 2020) en voortgangsrapportage NCSA (Kamerstuk 26 643, nr. 695);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 24 juli 2020 inzake rapport voortgang implementatie EU 5G toolbox (Kamerstuk 21 501-33, nr. 823);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 20 augustus 2020 inzake reactie op het verslag van de Inspectie Justitie en Veiligheid (IJenV) op het heimelijk en op afstand binnendringen in een geautomatiseerd werk (Kamerstuk 29 628, nr. 970);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 17 september 2020 inzake gegevens databestand Zhenhua (Kamerstuk 30 821, nr. 116);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 7 oktober 2020 inzake gijzelsoftwareaanval op Veiligheidsregio Noord- en Oost Gelderland (VNOG) (Kamerstuk 29 517, nr. 194);**

kst-28684-645
ISSN 0921 - 7371
's-Gravenhage 2021

- **de brief van de Minister van Justitie en Veiligheid d.d. 19 november 2020 inzake rapport «Informatie-uitwisseling landelijk dekkend stelsel cybersecurity» (Kamerstuk 26 643, nr. 717);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 30 november 200 inzake beantwoording vragen commissie over strategische afhankelijkheid buitenlandse partijen (Kamerstuk 30 821, nr. 121).**

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

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

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
Ziengs

De voorzitter van de vaste commissie voor Economische Zaken en Klimaat,
Renkema

De griffier van de vaste commissie voor Justitie en Veiligheid,
Haveman-Schüssel

Voorzitter: Van Meenen
Griffier: Schoor

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

en de heer Grapperhaus, Minister van Justitie en Veiligheid.

Aanvang 14.31 uur.

De **voorzitter**:
Goedemiddag. Van harte welkom bij deze vergadering van de vaste commissie voor Justitie en Veiligheid met als volgcommissies de commissie voor Binnenlandse Zaken en die voor Economische Zaken en Klimaat. Aan de orde is het algemeen overleg over cybersecurity. Ik heet de Minister en zijn ambtenaren van harte welkom. Dat geldt ook voor de leden en onze ondersteuning en de mensen die dit debat elders zullen volgen. Wij hebben afgesproken dat dit debat gaat duren tot uiterlijk 17.30 uur. Dat betekent dat we spreektijden hanteren van vier minuten. Ik zal gezien het aantal deelnemers tot nu toe niet op voorhand een grens stellen aan het aantal interrupties, maar ik ken u goed genoeg. Als u zich daarin kunt vinden, dan geef ik als eerste het woord aan mevrouw Buitenweg van GroenLinks.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, meneer de voorzitter. Fijn dat we dit AO toch kunnen hebben. Het was aanvankelijk omgezet in een schriftelijk overleg, maar ik denk dat dat geen recht doet aan het belang van het onderwerp. Het is goed dat wij om de paar maanden toch echt stilstaan bij dit onderwerp. Ik heb een paar punten. Ik ga er maar snel en wat staccato doorheen.
Ten eerste. In heel veel van de stukken wordt onderscheid gemaakt tussen vitale en niet-vitale sectoren. Dat zie ik ook in de stukken terug van het kabinet. Maar we hebben de afgelopen maanden met veel mensen gesproken, mevrouw Yeşilgöz en ik ook namens de JenV-commissie als een soort rapporteurs. We zien dat steeds meer mensen tegen ons zeggen dat dat onderscheid niet echt meer heel erg actueel is. Daarom is ook de vraag aan de Minister: wat is op dit moment nog de betekenis van het maken van onderscheid tussen vitaal en niet-vitaal? Gaat het niet eerder om vitale en niet-vitale ketens in plaats van sectoren? Wat is nu het gevolg van het feit dat de Minister dat onderscheid toch nog wel veel blijft maken, bijvoorbeeld voor de informatiedeling, maar misschien ook op andere gebieden. Dat hoor ik dus graag.
Ik vraag me ook af hoe hij bijvoorbeeld de zorg ziet en zorgaanbieders. Ik begrijp dat die gezien wordt als een niet-vitale sector op het gebied van cyberveiligheid. Ik vraag of hij toch zou willen benadrukken dat dit wel zo is, gezien het feit dat steeds meer ziekenhuizen ook met elkaar verbonden zijn. Wat betekent dat dan voor uiteindelijk de hele sector, die dan toch plat kan komen te liggen?
Ik heb begrepen dat er een plicht komt voor rijksoverheidsorganisaties van «pas toe of leg uit» met betrekking tot de adviezen van het NCSC. Gaat dit nu ook gelden voor private vitale aanbieders of niet? Ik las namelijk ergens dat de Minister voorlopig daarmee niet verder wilde gaan dan het maken van werkafspraken. Nou, dat vind ik vrij vrijblijvend klinken. Dus misschien kan hij toelichten of de «pas toe of leg uit»-plicht ook wordt uitgebreid naar private partijen en, zo nee, waarom niet.
Dan de ransomware. Daar hebben we de afgelopen weken ook weer veel voorbeelden van gezien. Natuurlijk gaan individuele organisaties wegen of het nou de moeite waard is om losgeld te betalen of niet. Dat is dus een soort individuele keuze, maar het belonen van misdaad is natuurlijk ook een zorg voor de hele samenleving, voor ons met z'n allen. Dat is eigenlijk

dus een soort externaliteit. Bij zo'n individuele beslissing wordt misschien niet altijd genoeg het perspectief van de hele samenleving betrokken. De vraag is of de overheid dan niet nauwer betrokken moet zijn bij afwegingen om losgeld te gaan betalen. Ik zag dat ze er in de Verenigde Staten over denken om die kant op te gaan. Mijn vraag is of het kabinet dat ook wil overwegen.

De **voorzitter**:
U heeft nog 50 seconden.

Mevrouw **Buitenweg** (GroenLinks):
O, heel snel dan. We praten ook vaak over onbetrouwbare leveranciers op cruciale plekken. We hebben het eerder gehad over Huawei. Maar dan gaat het nadenken natuurlijk heel erg over het hier en nu. Tegelijkertijd moeten we er natuurlijk vooral ook over nadenken hoe we ervoor zorgen dat onze ketens betrouwbaar zijn en dat we ook in de toekomst betrouwbare leveranciers hebben. Hoe brengen we die in positie? Daarvoor moeten we dus – dat zal dan het pleidooi van GroenLinks zijn – ervoor zorgen dat er voldoende Europese bedrijven zijn die dat ook kunnen leveren. Mijn vraag is: op welke wijze wil het kabinet dat gaan bevorderen? Klopt het dat departementen op dit moment allemaal apart databeveiligingsproducten inkopen? Wat zou daarvan de reden zijn? Is de Minister bereid om te koersen op veel meer centrale regie met centrale inkoop?
Ten slotte wil ik er nog voor pleiten dat er meer getest gaat worden in de werkelijkheid, dus niet alleen per kleine organisatie in de zin van: wat als daar een probleem is met een cyberaanval? Het gaat er natuurlijk om wat dat betekent voor de hele keten. Wordt er ook op die manier getest? Ik begrijp dat er een belangrijke crosssectorale oefening op cybergebied is, ISIDOOR, die eens in de paar jaar plaatsvindt en in 2020 zou moeten hebben plaatsgevonden. Is er nu al een nieuwe datum? Ik denk dat het echt van belang is dat we blijven testen en dan vooral op wat het voor de hele keten in de praktijk betekent. Wat zijn dan de mogelijkheden, ook in de fysieke wereld, om de problemen op te vangen?
Dank u wel.

De **voorzitter**:
Ik dank u zeer. Het woord is aan mevrouw Yeşilgöz van de VVD.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Dank u wel, voorzitter. Dit is een van de zeldzame onderwerpen waarbij mijn spreektekst bijna helemaal overeenkomt met de spreektekst van mijn collega van GroenLinks, maar ik ga toch even kijken of ik wat VVD-accenten kan aanbrengen. Nee nee, Minister, niet zo blij kijken; ik ga het toch proberen.
Als we heel eerlijk zijn, weten we allemaal dat het ontzettend belangrijk is om onszelf digitaal te beschermen, maar dat dit onderwerp niet altijd de urgentie heeft die het zou moeten hebben. Ook het aantal hier aanwezige woordvoerders zou daar misschien iets over kunnen zeggen. Een pijnlijk voorbeeld daarvan is de zeer recente immense vernietigende hack waardoor de gemeente Hof van Twente is getroffen. In een paar media konden we er wat over horen en lezen, maar dat was het eigenlijk ook wel, terwijl de impact enorm is. Uitkeringen, e-mails, vergunningaanvragen en andere persoonlijke gegevens van de 35.000 inwoners van de gemeente zijn gegijzeld door cybercriminelen. Als Hof van Twente de gegevens ooit nog terug wil zien, zal de gemeente moeten betalen. Ik meen dat het nu gaat om een eis van ruim € 750.000. De burgemeester van deze gemeente reageerde de eerste dagen na de hack zeer lauw. Ze leek zich niet bewust te zijn van de urgentie. Inmiddels lijkt iedereen wakker en alert, maar hier valt dus wel een wereld te winnen.

Deze vorm van criminaliteit is niet nieuw. We zagen het recent onder andere ook bij de Universiteit Maastricht. Het is helaas niet altijd te voorkomen, maar als we zo doorgaan, wanen criminelen zich onaantastbaar en wordt de kans op digitale ontwrichting steeds groter. Ik wil graag van de Minister weten hoe onze gemeenten beschermd zijn. Zijn er een helder protocol en een crisisplan? Is er duidelijkheid wanneer deze moeten intreden en dergelijke?
Daarmee zijn we er natuurlijk nog niet. Onze digitale veiligheid loopt in het algemeen achter op onze snelle digitale ontwikkeling. Wat de VVD betreft moeten we dat tij keren en serieus aan de slag gaan met hoe we onszelf digitaal beter kunnen beschermen. Dat begint bij de belangrijkste sector: de vitale infrastructuur. Denk aan elektriciteit, toegang tot internet, drinkwater en betalingsverkeer. Een uitval kan vergaande gevolgen hebben voor onze samenleving en daar moeten we op voorbereid zijn. Maar ondanks een aangenomen motie van de VVD en een oproep van vitale bedrijven zelf is er nog steeds geen structureel digitaal crosssectoraal oefenprogramma om te oefenen met digitale uitval. Wanneer kunnen we dit verwachten? Ik sluit me op dit punt aan bij de vragen van GroenLinks. En hoe staat het met de aangenomen motie van VVD en D66 over het scannen van kwetsbaarheden in overheidssystemen in de vitale infrastructuur? Gebeurt dit inmiddels?
Voorzitter. Ook de digitale veiligheid van ondernemers staat onder druk. Corona heeft hier nog een schepje bovenop gedaan. De vraag is of de Minister deze zorgen ook deelt. Mkb'ers krijgen nauwelijks informatie en ondersteuning bij digitale aanvallen omdat het Digital Trust Center nog steeds geen wettelijke status heeft om dreigingsinformatie te kunnen ontvangen van het Nationaal Cyber Security Centrum. Wat is volgens de Minister de verklaring voor het achterblijven van het landelijk dekkend stelsel? Waar ligt dit aan? Wat moet er volgens de Minister gedaan worden om in de toekomst vertraging te voorkomen en om daadkrachtiger aan de slag te gaan?
Voorzitter. Cybersecurity is niet alleen het beschermen van onze digitale infrastructuur, maar ook het tegengaan van bijvoorbeeld onlinefraude, -oplichting en -hatespeech zoals antisemitisme en racisme. We moeten voorkomen dat er online een soort vrijplaats ontstaat waar criminelen zich onaantastbaar wanen. Ik wil vandaag heel even focussen op de onlinespeech. Over andere elementen, zoals fraude, hebben we het onlangs al gehad. Welke concrete stappen neemt de Minister momenteel om onlinespeech tegen te gaan?
Voorzitter. Ten slotte wil ik stilstaan bij onze autonomie. Hoe beschermen we onze vrijheden en onze democratie tegen buitenlandse mogendheden die ons digitaal willen aanvallen of beïnvloeden? Vanuit het kabinet ligt een integrale aanpak voor om te bouwen aan de weerbaarheid tegen statelijke dreigingen. Als ik het goed heb begrepen, wordt onder coördinatie van de Minister van JenV bezien of alle betrokken partijen in ons land voldoende zijn toegerust om de dreiging het hoofd te bieden. Ik zou graag willen weten wat de stand van zaken daarvan is.

De **voorzitter**:
Ik dank u zeer. Er is een interruptie voor u van mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
We zijn het grotendeels eens, de VVD en GroenLinks. Ik hoop over het volgende wat ik ga vragen ook. Wellicht wel. Dat gaat over hoe wij wat meer kunnen bevorderen dat wij een soort Europese industriepolitiek gaan voeren waarmee wij er op de langere termijn voor zorgen dat wij toeleveranciers krijgen die wij echt kunnen vertrouwen. Is de VVD bereid om ook op Europees niveau na te denken over voorstellen om Europese bedrijven een extra stimulans te geven ten opzichte van wellicht andere bedrijven?

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Ik denk dat wij het in de basis eens zijn. Wat de invulling en uitvoering betreft zou het best kunnen dat GroenLinks en de VVD toch een beetje uit elkaar liggen, maar de urgentie in de oproep begrijp ik. De autonomie waar ik het aan het einde van mijn betoog over gehad, is niet alleen gericht op Nederland maar ook op onze Europese samenwerking en waarden. Eigenlijk gaat het over die beide zaken. Hoe zorg je ervoor dat je dat overeind houdt en goed beschermt? Over de bescherming en de invulling daarvan zouden wij van mening kunnen verschillen, maar laten we ervan uitgaan dat wij in de basis dezelfde zoektocht delen.

Mevrouw **Buitenweg** (GroenLinks):
Ik weet niet waar we in de invulling dan precies verschillen, maar ik denk dat het belangrijk is om te zeggen dat het dus niet alleen over Nederland gaat. Het valt mij op dat Nokia en Ericsson heel erg gezien worden als Fins of Zweeds, maar uiteindelijk zijn het essentiële Europese bedrijven. Het is van belang om te kijken hoe wij kunnen stimuleren dat bij die bedrijven bepaalde privacy- of andere standaarden kunnen worden ingebouwd, dat die meer de norm worden, zodat dat veel meer, om het even plat te zeggen, een opkontje krijgt.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Daar kan ik me gewoon bij aansluiten. Internet en cyberveiligheid houden niet op bij de landsgrenzen. Corona heeft ons het afgelopen jaar heel veel lessen geleerd in die zin dat je heel goed moet kijken hoe je in Europa goed kunt samenwerken om je autonomie en bepaalde zaken omhoog te houden.

De **voorzitter**:
Ik dank u zeer. Dan is het woord aan de heer Van Dam van het CDA.

De heer **Van Dam** (CDA):
Voorzitter. Uiteraard sluit ik me aan bij de inbrengen van de vorige sprekers als het gaat om de situatie in de gemeente Hof van Twente. Ik heb vandaag toevallig nog contact gehad met de burgemeester. Ik denk dat die burgemeester het prima onder controle heeft, althans gegeven de omstandigheden. Wij moeten het bestuur daar steunen in hun aanpak.
Ik wilde een ander punt benadrukken als het gaat om cybersecurity en dat is de burger. Ik heb laatst een nieuw begrip geleerd: PEBKAC. Dat is een begrip dat in de IT wat honend genoemd wordt. Het is de afkorting van problem exists between keyboard and chair. Dat komt er eigenlijk op neer dat het grote probleem bij cybersecurity of bij cyberonveiligheid de mens is, hè, tussen stoel en toetsenbord. Ik denk dat dat voor een belangrijk deel waar is. Wij besteden terecht heel veel aandacht aan het vitale niveau, via NCSC en andere instellingen. Wij besteden tegenwoordig via het Digital Trust Center ook veel aandacht aan andere niveaus: het midden- en kleinbedrijf en andere sectoren. Maar wat heeft de burger nou aan informatie en welk handelsperspectief heeft hij? Naar mijn smaak is dat betrekkelijk weinig.
Ik heb de vraag laatst ook gesteld in een briefing van de Cyber Security Raad: wordt het niet tijd dat we in Nederland eens wat meer gaan doen aan een cyberweerbericht? Dat hoeft voor mij niet iedere avond na het achtuurjournaal uitgezonden te worden, maar zoals alle hooikoortslijders, waar ik er ook een van ben, gewaarschuwd worden voor een pollenstorm uit het noorden of een kudde zetmeel uit het zuiden, kan ik mij voorstellen dat de burger, de gebruiker van digitale middelen, gewaarschuwd wordt voor een nieuwe phishinggolf die er via bank X of Y aankomt of voor gevaar dat hij loopt via zijn postorderbedrijf of hoe dat tegenwoordig ook heet, en dat hem verteld wordt wat hij dan moet doen. Ik wil de Minister

vragen om daar eens op te reageren. Zou hij willen onderzoeken wat daar mogelijk is? Daar zijn goede voorbeelden van in andere Europese landen.
Voorzitter. De coronacrisis. Onze afhankelijkheid van digitale middelen is nog nooit zo hoog neergezet als op dit moment. Natuurlijk zien we angstwekkende voorbeelden, zoals bij de Universiteit Maastricht en nu in een gemeente. Zou de Minister eens kunnen reflecteren op wat er in het kader van de coronacrisis op dit moment is aan digitale paraplu, digitale bescherming? De komende feestdagen gaan we met z'n allen digitaal op bezoek bij schoonmoeder en nichten en neven. Dat wordt nogal wat. Hoe kwetsbaar zijn we en hoe worden we beschermd? Zijn daar met de providers afspraken over gemaakt?
De Minister heeft een mooie brief geschreven over internetcriminaliteit. Ik zie daar een zekere spanning in. Enerzijds zegt hij dat we dingen in Europees verband samen met grote internationale platforms en diensten-aanbieders gaan doen. Tegelijkertijd zie ik dat de aanpak van kinderporno vooral een Nederlandse oriëntatie heeft. Ik ben er overigens zeer tevreden mee dat de Minister daar zo veel werk van maakt. Ik vroeg me af wat er in Europees verband wordt gedaan tegen de bestrijding van kinderporno. Ik haal dat gewoon niet zo uit de brief. Als ik het gezicht van de Minister zie, krijg ik de indruk dat hij daar goede antwoorden op gaat geven zo dadelijk. Die wil ik heel graag horen.
Verder wordt er erg gekoerst op die HashCheck als een middel om de foute foto's uit de stapel te halen. Ik heb mij laten vertellen dat je al een heel andere HashCheck hebt, als je maar een bitje aan zo'n bestand, zo'n foto, verandert. Wordt daarin voorzien? Die boeven zijn toch vaak slimmer dan de hele Haagse politiek bij elkaar, terwijl wij toch ook ongelofelijk slim zijn. Wat is de inschatting van de Minister hiervan?

De **voorzitter**:
Kunt u afronden?

De heer **Van Dam** (CDA):
Ik ga afronden, zeker. Tot slot. Er liggen een aantal rapporten van de Algemene Rekenkamer. Een daarvan gaat over de grenscontrolesystemen op Schiphol. In dat rapport is ook te lezen dat dat grenscontrolesysteem overgedragen gaat worden aan de particuliere Schiphol Group, dus dat het uit de macht van de marechaussee of de douane gaat en dat het systeem beheerd gaat worden door de Schiphol Group. Daar heb ik toch wel een vraag over. Zouden we dat nou moeten willen? Want mij lijkt dat toch ook een vitaal systeem. Graag een reactie van de Minister.

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

De heer **Verhoeven** (D66):
Voorzitter, dank u wel. De afgelopen jaren heeft D66 op het gebied van digitalisering en datatechnologie verschillende voorstellen gedaan, soms met steun van de Kamer. De uitvoering door het kabinet laat hier en daar nog wel wat te wensen over. Ik stel de Minister dus nu maar gewoon directe vragen. Allereerst: staat de Minister vanaf nu pal voor encryptie, versleuteling? Gaat het kabinet nog komen met iets dat lijkt op een ambitieus deltaplan cybersecurity? Hoe gaan we op Europees niveau eisen stellen aan buitenlandse leveranciers? Dat zijn voor mij vandaag even de drie belangrijkste vragen na vier jaar digitalisering bij Justitie en Veiligheid. Er is veel gebeurd. Ik vond het ook aardig om te horen dat de collega zei: misschien zijn we het hier dan wel een keer allemaal over eens. Dat gevoel heb ik ook al een tijd. Dat lijkt en comfortabel, maar dat is eigenlijk ook wel een teken dat het debat misschien nog niet volwassen is, dat dingen nog niet duidelijk genoeg uitgekristalliseerd zijn en dat we dus in algemene termen over iets praten waarvan we denken dat we het

erover eens zijn, maar dat blijkt dat er verschillen zijn, als we het preciezer gaan zeggen.
Dat zou bijvoorbeeld weleens kunnen gelden voor een onderwerp als versleuteling. Ik wil daar toch wat vragen over stellen. Er gingen voor de zoveelste keer in deze kabinetsperiode geruchten over het verzwakken van versleuteling, over het inbouwen van bepaalde achterdeurtjes, al dan niet op Europese Raadsniveau. Het ging om «technische oplossingen». Kan de Minister toelichten welke technische oplossingen in Europa zijn besproken als het gaat om versleuteling? Is de Minister het eens met D66 dat een achterdeur door iedereen en dus ook door kwaadwillenden gebruikt kan worden? Dan verliest encryptie zijn nut. Hoe kun je nou een fundamenteel recht als privacy beschermen als je niet meer in onderling vertrouwen kunt communiceren? Hoe is het mogelijk dat er daarvoor steun is geweest? Of laat ik het zo vragen: kan er steun zijn voor de Raadsresolutie ten opzichte van het kabinetsstandpunt uit 2016 waarin gewoon staat dat Nederland voor sterke encryptie is? En tot slot: hoe kunnen journalisten, mensenrechtenactivisten, advocaten en medici met elkaar communiceren op het moment dat ze niet zeker weten of er iemand meekijkt? Dat waren mijn eerste vragen over het onderwerp encryptie.
Dan kom ik op de vitale infrastructuur. De heer Van Dam is onnavolgbaar, maar ik zie dat hij eerst een vraag aan mij heeft.

De heer **Van Dam** (CDA):
De heer Verhoeven doet eigenlijk een soort appel om daarover in debat te komen. Dat kan met de Minister, maar mij is de gelegenheid geboden om daar ook als Kamerlid over in debat te gaan. Ik moet zeggen dat ik zelf de afgelopen periode ook wel een weg ben gegaan in mijn oordeel over het punt encryptie. In principiële zin heb ik er helemaal niets op tegen, want we kunnen ook telefoongesprekken aftappen en woonkamers binnen komen om mensen af te luisteren. Dat is wettelijk geregeld. Maar wat betreft de technische effecten die dit kan hebben en het niet zeker kunnen weten dat je niet andere mensen binnenlaat, zijn er meer waarborgen bij een woonkamer en een telefoongesprek dan bij dit onderwerp. Dat heeft bij mij geleid tot de gedachte dat het misschien niet slim is om dit te doen. Maar ik wil toch eens aan de heer Verhoeven vragen of hij mij dat principiële punt na spreekt, namelijk dat er in principe geen verschil zit tussen het aftappen van een telefoongesprek of het meeluisteren van een chatgesprek, maar dat je het verschil meer in de techniek moet maken?

De heer **Verhoeven** (D66):
Dat is een mooie vraag en een mooie open afweging van de heer Van Dam. Hij geeft aan dat hij een weg heeft afgelegd in zijn denken. Ik ken de heer Van Dam ook niet anders dan iemand die voortdurend wegen aflegt in zijn denken. Ik vind dat heel positief. Ik zal dan ook open tegen hem zijn. We hadden hier afgelopen maandag ook een debat over een middel om een doel te bereiken. In die zin zou ik het antwoord willen geven. Het middel is dan de weg die je loopt om het doel te bereiken. Over het doel zijn we het eens. Het middel is hier technisch en heeft als principiële consequentie dat je niet kan garanderen dat het zich beperkt tot die kleine telefoonlijn of huiskamer. Het technische middel maakt dus de principiële afweging anders, omdat je hier niet kunt garanderen dat het zich niet breder uitstrekt dan alleen maar tot de persoon die je wilt afluisteren. Door de techniek moet je hier dus een principiële keuze maken, namelijk dat het buitenproportioneel is om een opening te maken waar iedereen doorheen kan. Daarom ben ik zo kritisch over het verzwakken van encryptie.

De heer **Van Dam** (CDA):
Dat is voor mij een heel helder antwoord op mijn vraag, want daarmee hoor ik de heer Verhoeven dus zeggen dat hij geen principieel bezwaar

zou zien, als het technisch wel zou kunnen. Dat is heel goed. Dat is een positieve reactie, vind ik. Dan kan ik nu de heer Verhoeven de ruimte geven om wat kritischer te zijn op een ander punt van mijn inbreng, want ik hoorde al de opmaat.

De heer **Verhoeven** (D66):
Nou, ik had eigenlijk iets heel aardigs voor u in gedachten. Daar blijf ik ook bij. Maar ik wil wel nog even iets over uw samenvatting zeggen. Kijk, dit doen we vaal in de politiek: u zegt dit, dus u bedoelt dat en daarmee kunnen we verder, want... Ik heb heel lang en heel vaak over dit onderwerp nagedacht. Op dit moment is het zo dat mij geen enkele mogelijkheid bekend is om een softwarekwetsbaarheid te gebruiken op een manier die zich beperkt tot het target om het te doen. Dat betekent dat je het dus niet gericht kunt inzetten. Doordat je het niet gericht kunt inzetten, is het dus een ongericht middel. Daarmee is het dus ook een principieel onwenselijke weg. U vraagt: mocht er ooit een manier bestaan om dat wel te doen, hoewel die er nu niet is, wat dan? Dan is het wat mij betreft aan mij om dan in mijn denken de wegen af te leggen die de heer Van Dam de afgelopen tijd heeft afgelegd. Zo zou ik het willen samenvatten.

De **voorzitter**:
Ik begrijp het. Er is ook nog een vraag voor u van mevrouw Buitenweg.

De heer **Verhoeven** (D66):
Nou is het hek van de dam, voorzitter.

Mevrouw **Buitenweg** (GroenLinks):
Het is in dit geval een oprechte vraag. Ik stel de vraag aan de heer Verhoeven, maar ik hoop dat ook de Minister daarop wil reflecteren. Dit is een onderwerp waarop ik het antwoord juist nog niet heb. Het is dus echt een vraag. Het gaat over het internet. De internetprotocollen worden vastgesteld via het multistakeholderprincipe. Wat moet de rol van Nederland daarin zijn? China wil een nieuw IP voorstellen via de International Telecommunication Union. Is dat iets waar we bang voor moeten zijn? Waar zou dat moeten worden vastgelegd? Is dit iets waar in het idee van de heer Verhoeven voldoende beleid op ontwikkeld is of zou moeten zijn? Hoe ziet hij de rol van de Staat in deze enorm veel organisaties met heel veel afkortingen?

De heer **Verhoeven** (D66):
Ik weet hier helemaal niet zo heel veel van af, althans ik ken de protocollen die ten grondslag liggen aan de werking van het internet en de manier waarop ze tot stand gekomen zijn. Maar de laatste ontwikkelingen ken ik ook niet precies. Een jaar of zes geleden is er wel een prachtig rapport verschenen dat ging over de publieke kern van het internet. Kent u rapport, voorzitter? Ik denk dat het een rapport is van de WRR: De publieke kern van het internet. Dat gaat exact over deze vraag en over het feit dat er eigenlijk geleidelijk van onderaf wat meer wetenschappelijk-private protocollen zijn ontwikkeld die hebben geleid tot het internet. Eerst zeiden de overheden: daar gaan we niet over. En vervolgens zijn ze allemaal manier gaan bedenken om het internet te controleren: securitization. Nu is het de vraag wat staten moeten doen ten opzichte van die ontstane protocollen. Soms worden die protocollen door hobbyisten waarop iedereen leunt in zijn communicatie, bijgehouden, zonder dat deze mensen daar geld voor krijgen. De publieke kern van het internet is een heel goed rapport daarover. Volgens mij is de lijn van dat rapport nog steeds heel actueel, namelijk dat landen een heel voorzichtige en internationaal samenwerkende houding moeten aannemen en dus niet

allerlei eisen moeten gaan stellen. Eigen internetjes, de balkanisering van het internet heet dat, moeten we niet doen. Dat weet ik in ieder geval wel.

De **voorzitter**:
Mevrouw Buitenweg nog.

Mevrouw **Buitenweg** (GroenLinks):
Ik kan me het antwoord goed voorstellen, want ik ben ook heel huiverig voor een grotere invloed van overheden daarop, omdat dat juist ook een gevaar kan zijn voor het vrije internet, denk ik. Tegelijkertijd zijn er op dit moment natuurlijk ook juist bedrijven die vooral weer tot doel hebben dat de diensten verbeterd worden. Dat is nog iets anders dan dat de mensenrechten gediend zijn. Dat is waar ik me zorgen over maak. Wordt er, wanneer er nieuwe voorstellen komen, voldoende gekeken naar de impact op mensenrechten? Hoe kunnen we dat waarborgen? Maar misschien is dat iets waar we de Minister later ook nog op kunnen bevragen.

De heer **Verhoeven** (D66):
Dit is een superbelangrijk onderwerp. Op dit moment gaat dat ook mijn reikwijdte te boven, maar de verhouding tussen burgers, Staat en bedrijven en de rol van het internet daarin is een machtige vraag. Als je het nou hebt over wel of geen censuur, dan is de vraag ook: we hebben nu censuur van techbedrijven; moeten we dan censuur van staten hebben? Moet de Staat controle over het internet hebben? Dan denken we gelijk aan Turkije en Rusland. Nee, dat willen we niet. Maar moeten techbedrijven dan allesbepalend zijn? Nee, ook niet. Moet de Staat dan gaan interveniëren? Ja, misschien wel. De vraag is dan hoe. Het is dus een superingewikkelde vraag. De Minister zal daar dadelijk vast wel een kernachtig betoog over houden met een aantal steekhoudende argumenten, maar ik kan dat nu in ieder geval niet meer dan ik heb geprobeerd.

Mevrouw **Buitenweg** (GroenLinks):
Ik kijk uit naar het vervolg.

De **voorzitter**:
We kijken ernaar uit. Meneer Verhoeven, gaat u verder. Of was u al klaar?

De heer **Verhoeven** (D66):
Nee. Dat zou u wel willen, voorzitter, maar de heer Van Dam... Ik heb heel lang gedacht – ik maak nu een stapje naar de vitale infrastructuur – dat we het moesten hebben over cyberweerbaarheid. Nu zegt de heer Van Dam: nee, we moeten het hebben over een cyberweerbericht. Aan de ene kant vind ik dat grappig, maar aan de andere kant is dit een supergoed en concreet voorstel. Want er is inderdaad wel wat aan de hand als het gaat om de positie van de burger en de veiligheid van communiceren. Een weerbericht waarin bijvoorbeeld bekend wordt gemaakt welke hackaanvallen en welke phishingmails er zijn, welke sectoren kwetsbaar zijn en welke bedrijven onder druk staan, zou best weleens een aardig idee kunnen zijn. Ik zou de heer Van Dam daar dus eigenlijk in willen bijvallen. We hebben namelijk gezien dat 112, waterwerken, betalingsverkeer en elektriciteit allemaal cruciale onderdelen zijn van onze infrastructuur. De burger begeeft zich daar dagelijks in. Waarom zouden we dan niet een beetje helpen door hem te informeren over de laatste dreigingsbeelden? Voorzitter. Ik heb weleens vaker het boek van Huib Modderkolk en die 340 miljoen genoemd. Op basis daarvan heb ik ooit een keer aan de Minister gevraagd: goh, wat gaan we nou doen om genoeg te investeren in cybersecurity? Toen was de Minister in een goede bui. Hij zei: nou, weet je, ik doe de heer Verhoeven een toezegging; ik ga ervoor zorgen dat we gaan kijken wat de benodigde investeringen zijn om Nederland op een

afdoende niveau veilig te houden. Mijn vraag is dus: hoe staat het met dat onderzoek?
En hoe staat het met de Europese minimumeisen voor IoT-producten? Dat is mijn volgende onderwerp. D66 is er voorstander van dat Europa markteisen stelt aan IoT-apparaten. Worden daar stappen in gezet?
Voorzitter. Dan de organisatie en het deltaplan cybersecurity. Ik moet opschieten, begrijp ik?

De **voorzitter**:
Nou...

De heer **Verhoeven** (D66):
Dat doe ik. Naast het geld is er ook een organisatieslag nodig. Ik geloof dat mevrouw Yeşilgöz dat ook al zei. Hoe staat het met de motie van mevrouw Laan-Geselschap en mij over het scannen?
Tot slot de bevoegdheden van het Nationaal Cyber Security Centrum. Die zouden wat D66 betreft moeten worden uitgebreid om ervoor te zorgen dat het NCSC die brandweercommandantrol kan nemen die ook in het WRR-rapport over digitale ontwrichting naar voren kwam.
Voorzitter. Als allerlaatste punt de Europese samenwerking. Het op magere gronden weigeren van Kaspersky, het twijfelen over een exportvergunning voor ASML en het hoofdpijndossier 5G laat zien dat we op Europees niveau knopen moeten doorhakken in deze cyberstrijd tussen de VS, China en Europa. Hoe gaat de Minister dat verder stimuleren?

De **voorzitter**:
Dank u zeer, meneer Verhoeven. De Minister heeft verzocht om een kwartier schorsing. Die ga ik hem geven. Wij gaan dus iets na 15.15 uur van start.

De vergadering wordt van 15.01 uur tot 15.18 uur geschorst.

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

Minister **Grapperhaus**:
Ik heb twee powerpoints van 30 bladzijden!
Voorzitter. Ik houd ervan als ik kan beginnen met direct tegen uw Kamer te zeggen dat we altijd goede, kritische debatten voeren. Ik vind het heel bijzonder dat we die kritische debatten, bijna volgens het principe van de wonderbaarlijke broodvermenigvuldiging, nu ook over cybersecurity met meer dan twee Kamerleden voeren. Dat is een goede zaak.
Voorzitter, ik heb voor u iets meegenomen. Het is minder dan € 50; ik heb het prijsje erop laten zitten. Wellicht kunt u het delen met de commissieleden, want dit boek heeft mij op een aantal punten aangegrepen, ook persoonlijk in het relaas van Daniël Verlaan. Het is het boek Ik weet je wachtwoord. Dit is een belangrijk iets wat op microniveau symbool staat voor cybersecurity, want cybersecurity begint gewoon bij ons allemaal aan de keukentafel. Ik geef het heel eerlijk toe, ik ga het nu echt gewoon zeggen: in de eerste jaren van het internet waren mijn favoriete wachtwoorden «Ferd1959» en «1959Ferd». Ja, het geboortejaar en de voornaam. Dat is niet heel handig en daar kom je dan ook wel snel achter. Maar hier gaat natuurlijk veel meer achter schuil. Daarom wil ik dit boek, zo vlak voor het reces, aan u aanbieden.

De **voorzitter**:
Veel dank. Ik zal zorgen dat de hele commissie dit leest.

Minister **Grapperhaus**:

Voorzitter. Ik ga direct door naar de antwoorden. Ook de zeer kritische opmerkingen van mevrouw Buitenweg neem ik graag ter harte, maar ik vind het echt goed dat we deze discussie voeren. Cybersecurity is een lastig onderwerp. Het is voor veel mensen niet sexy. Het wekt bij mensen toch te weinig de associatie op dat als we in het analoge leven allerlei veiligheidsvoorzieningen treffen, we dat ook echt in het digitale leven moeten doen. Dat is ook omdat we in het analoge leven nooit zo gewend waren om zo veel dingen te delen, om zo veel dingen te communiceren, om zo veel dingen open te zetten. Wij als bevolking, maar ook de instituties, de overheid... Daarom is het ook goed, ik kom daar zo als een van de eerste punten op, dat we het even over Hof van Twente en dat soort zaken gaan hebben.
Ik ben nu iets meer dan drie jaar in deze functie en dit is echt een onderwerp waarvoor we voortdurend aandacht moeten blijven vragen. Ik zeg het wat bitter: ik denk dat er in ons land nog steeds meer aandacht voor nodig is, veel meer dan er nu voor is. De gemiddelde ophaalbrug bij de Friese meren is niet meer analoog te bedienen. Het gaat allemaal op basis van digitale technologie. Terecht vroeg de heer Verhoeven aandacht voor de «Internet of Things»-apparatuur. Je moet er niet aan denken dat iemand op afstand al die geautomatiseerde temperatuurkastjes gaat gebruiken, of hoe heten die dingen in huis? Thermostaten; ik heb een open haard, vandaar. Ja, dat is heel slecht voor het milieu, maar het is een gashaard. Die kan ik binnenkort dus ook afsluiten.
Voorzitter. Ik ga concreet op de vragen in. Ik begin bij de vragen van mevrouw Buitenweg. Soms is er een doublure met andere vragen, maar ik heb, afwijkend van mijn patroon, de onderwerpen niet gebundeld. Omdat u nu met z'n vieren bent, dacht ik: ik doe het zo veel mogelijk per persoon. Mevrouw Buitenweg en mevrouw Yeşilgöz vroegen beiden naar het oefenen en testen. Het oefen- en testprogramma heb ik laten ontwikkelen, ook naar aanleiding van de motie van Arne Weverling, lid van de VVD. Dat programma is inmiddels ook in gebruik genomen. Voor oefenen zijn drie sporen uitgezet, die in de voortgangsbrief over de Nederlandse Cybersecurity Agenda 2020 staan. Ik vat het hier kort samen en verwijs verder naar die brief. Het bestaat uit het organiseren van oefeningen in het kader van het Nationaal Crisisplan Digitaal, zoals de grote oefening met de omineuze naam ISIDOOR, het deelnemen aan bestaande oefeningen in verschillende sectoren, zoals Cyber Europe en ddos-oefeningen, en tot slot het ontwikkelen van initiatieven in publiek-privaat verband, zoals via de Cybersecurity Alliantie. Specifiek voor het testen heeft Nationaal Cyber Security Centrum een whitepaper over securitytesten gepubliceerd in maart 2020. Bovendien heeft het DTC informatie gepubliceerd over testen op zijn website. Het is ook opgenomen in het basisnormenkader voor overheidslagen, de zogenoemde BIO. Over de voortgang van het oefen- en testprogramma zal ik uw Kamer jaarlijks informeren in de verdere voortgangsbrieven van de NCSA, zoals dit jaar ook is gebeurd. ISIDOOR gaat nog voor de zomer van 2021 plaatsvinden, in het tweede kwartaal. De voorbereidingen zijn in volle gang. Ik heb al eerder aan uw Kamer uitgelegd dat dat ten gevolge van alle coronabeperkingen op die tijd is gezet.
Terecht werd gevraagd of de overheid nauwer betrokken moet zijn bij de afwegingen om losgeld te betalen bij ransomware. Vanuit de overheid wordt bij ransomware altijd geadviseerd geen losgeld te betalen. Ik heb er naar aanleiding van de kwestie van de Universiteit Maastricht nog eens een brief over gestuurd aan uw Kamer. Ik weet dat het makkelijk praten is als je niet in die situatie zit, maar het doen van losgeldbetalingen houdt altijd het verdienmodel van ransomware in stand. Voor private bedrijven is dat overigens uiteindelijk een beslissing die zij zelf nemen. De vitale sector en de publieke sector vallen onder de NCTV als het om die afweging gaat. Dat betekent dus dat de NCTV, onder mijn politieke verantwoordelijkheid vallend, nauw betrokken is bij die afwegingen als

het om de vitale sector, de publieke sector gaat. Bij de private bedrijven zijn we bezig om dit dringende advies, dit motto, ook echt overal onder de aandacht te brengen. Maar goed, dat is uiteindelijk een afweging waar we niet, althans onder de huidige wetgeving, dwingend op in kunnen stappen.

Mevrouw **Buitenweg** (GroenLinks):
Ik begrijp de huidige situatie. We kunnen inderdaad op een gegeven moment gaan overwegen of het wel wat dwingender moet, maar dat is niet de situatie. Wat ik een probleem vind, is dat we op dit moment eigenlijk vrijwel niet in kaart hebben hoe vaak het nou voorkomt. Dat las ik in de antwoorden op de schriftelijke vragen: het kabinet vindt het betalen van losgeld onwenselijk, maar weet eigenlijk niet hoe vaak het voorkomt. Maar als we nou met zijn allen iets onwenselijk vinden, is denk ik het minste dat we moeten willen dat we er goed beeld hebben van hoe vaak het voorkomt. Dan kunnen we daarna nog besluiten of we toch vinden dat de afspraken daarop moeten worden aangepast. Op welke wijze wil het kabinet daar nou toch een beter beeld van krijgen?

Minister **Grapperhaus**:
Ik kom daar eigenlijk meteen aan toe als ik even die «pas toe of leg uit»-vraag van mevrouw Buitenweg bespreek. Laat ik dat eerst meenemen. De vraag van mevrouw Buitenweg was of dat nou ook voor de private vitale aanbieders geldt en of dat om een plicht gaat of om werkafspraken. Ik heb u gezegd dat ik werk aan verdere «pas toe of leg uit»-afspraken. Bij Citrix hebben we gewoon heel duidelijk gezien dat het van belang is om snel opvolging te geven aan beveiligingsadviezen van het NCSC. Daar stuitten we op problemen in de private en semi-private sector, omdat gewoon die adviezen niet direct werden opgevolgd. We werken nu aan werkafspraken om ervoor te zorgen dat in ieder geval de vitale aanbieders uitleg geven over de opvolging van HIGH/HIGH-beveiligingsadviezen, waarbij de prioriteit ligt bij het opheffen van de kwetsbaarheid zodat de vitale processen door kunnen gaan of in ieder geval niet in gevaar komen.
Een toezichthouder heeft ook de mogelijkheid om dwingender op te treden. Ik ben nu – dan ga ik weer terug naar het punt van daarnet van mevrouw Buitenweg – de mogelijkheden in kaart aan het brengen voor het wettelijk instrumentarium om daar in te kunnen grijpen tijdens een crisis. Ik kom begin volgend jaar met een brief daarover en ik wil dit punt van mevrouw Buitenweg daar meteen in meenemen: hoe kunnen we nou meer in beeld krijgen wat er in die private sector precies gebeurt? Als ik schrijf dat we dat niet precies in beeld hebben, is dat niet uit een soort van «wat gaat ons dat aan». Dan is dat omdat ik ook de zorg heb dat bedrijven niet altijd de melding doen waarvan wij zeggen: die moet je doen, zodat we weten wat er speelt. Ik wil geen – hoe noem je zoiets? – dode mussen, of wat dan ook – ik ben het even kwijt – verkopen.

De heer **Verhoeven** (D66):
Blij maken met een dode mus.

De **voorzitter**:
Ja, fijn. Hartelijk dank.

Minister **Grapperhaus**:
Ik vind dit geen interruptie, maar ik ga er niet over.

De **voorzitter**:
Zullen we die niet tellen? Nou, vooruit.

Minister **Grapperhaus**:

Ik wil u niet blij maken met een dode mus. Ik moet nog wel voor mezelf, in goed gesprek met de NCTV en met onze juristen, vaststellen wat je nou hiervoor kunt regelen in een wettelijk instrumentarium. Op het moment dat in de private sfeer bedrijven helemaal standalone, althans stand without de overheid, hun systemen draaien, kom ik ze pas tegen op het moment dat ze bijvoorbeeld zakendoen met de overheid. Dan is de vraag of je dit in aanbestedingsvoorwaarden mag opnemen en wat dies meer zij. Daar wil ik nu niet te veel op vooruitlopen. Ik wil alleen zeggen dat dit wel een complexiteit is in dit hele verhaal.

Mevrouw **Buitenweg** (GroenLinks):
Het is een complexiteit, maar de Minister maakt het er volgens mij niet makkelijker op. Ik heb het idee dat er nu verschillende dingen zijn. De vraag over het kunnen weten wat er aan de hand is, ging over het losgeld. Daarvoor kan je natuurlijk, althans in mijn ogen, wel degelijk een verplichting opleggen. Je zou dat kunnen overwegen. Dat is in ieder geval wat ik wil vragen aan het kabinet. Op welke wijze kunnen we nu beter in kaart krijgen wat bedrijven doen? Want bedrijven kunnen wel een eigen afweging maken, maar dat heeft uiteindelijk een enorm gevolg voor de hele samenleving. Want als heel veel bedrijven een individuele afweging maken om dan maar een paar ton te betalen, is dat voor hun misschien maar een paar ton, maar dan zijn we hele criminele netwerken aan het voeden. Bovendien leidt dat ertoe dat die weten dat ze vervolgens weer anderen zo kunnen chanteren. De impact is er dus voor de hele samenleving. Ik begrijp dat de Minister gaat kijken – dat gaan we dan in de brief zien, want hij weet nog niet wat de uitkomst is – of er mogelijkheden zijn en, zo ja, welke om hier toch een soort verplichting te hebben. Dat is een. Dat andere gaat over «pas toe of leg uit». Dat ging in mijn ogen over de eisen die gesteld werden voor de cyberveiligheid van producten. Ik begrijp dat de Minister daarover zegt dat de vitale sector daarin voorgaat. Begrijp ik dan goed dat dat geldt voor zowel de private vitale aanbieders als voor de publieke? Ik maak uit iets anders op dat hij bij de private vitale aanbieders niet verder gaat dan het maken van werkafspraken. Maakt hij bij die sector nou wel of niet een onderscheid tussen privaat en publiek?

De **voorzitter**:
De Minister, twee vragen.

Minister **Grapperhaus**:
Eerst even dit. Ik dacht dat ik de eerste vraag beantwoord had. Ik had gezegd dat je moet kijken wat de mogelijkheden zijn om de private sector tot een soort informatieverplichting te krijgen. Ik noemde als voorbeeld dat dat misschien zou kunnen via aanbestedingsvoorwaarden, dat je als je zakendoet afspreekt dat er volledige transparantie is over de systemen en problemen die daarin spelen. Er zijn misschien ook andere oplossingen mogelijk. Daar gaat de brief van begin volgend jaar over.
Dan het tweede punt: het onderscheid tussen vitale en niet-vitale sectoren. Daar vroeg mevrouw Buitenweg naar in de eerste termijn: kijkt u nou naar sectoren en niet naar ketens? Bepaalde processen zijn zo belangrijk voor de Nederlandse samenleving dat uitval of storing tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Dat noemen we de Nederlandse vitale infrastructuur. Daar ben ik uitvoeriger op ingegaan bij de mondelinge behandeling van het wetsvoorstel computercriminaliteit III en in de schriftelijke stukkenwisseling die bij dat wetsvoorstel aan de orde is geweest. Er wordt dan uitdrukkelijk gekeken naar vitale processen en ketens en niet zozeer naar sectoren. De beoordeling of een proces vitaal is, wordt gemaakt door het verantwoordelijke vakdepartement op basis van de opgestelde impactcriteria zoals economische schade en fysieke gevolgen.

U kunt zich misschien herinneren – ik zit even te kijken, volgens mij waren de meesten van u daarbij aanwezig – dat ik bij de behandeling van de Wet computercriminaliteit III uiteen heb gezet dat de Minister voor Medische Zorg destijds had ingeschat of gekwalificeerd dat bijvoorbeeld ziekenhuizen niet onder de vitale sectoren vielen, om op zichzelf heel goed beargumenteerde redenen. De Minister voor Medische Zorg heeft onlangs aan uw Kamer meegedeeld dat zij daar opnieuw naar zal kijken, naar de vraag of de zorg niet voor een deel of geheel vitaal moet worden verklaard. Dat was naar aanleiding van een motie van het Kamerlid Joba van den Berg van het CDA. Ik denk dat dat in ieder geval nog terugkomt.

De **voorzitter**:
Meneer Verhoeven. Sorry, mevrouw Buitenweg. Ik kom zo bij u terug.

De heer **Verhoeven** (D66):
Dit is een belangrijke discussie. Ik was laatst op werkbezoek bij het Cyber Emergency Response Team voor de zorg, Z-CERT, in Amersfoort. Dat is dus een CERT. Er zijn vier CERTs in Nederland: gemeenten, waterschappen, nog iets en zorg. De directeur van het Z-CERT gaf mij een rondleiding en vertelde wat ze deden. We hadden videovergadering met zijn team. Hij vertelde dat het eigenlijk heel goed geregeld is nu. Ondanks het feit dat de ziekenhuizen, de zorgsector, niet per definitie in de vitale infrastructuur zitten, is er wel een soort van verbinding gelegd via het Z-CERT naar het NCSC, waardoor de vitale informatie wel degelijk terechtkomt bij die zorginstellingen. Oftewel, er is een bypass, om het maar even die termen houden, gemaakt, waardoor het alsnog goed gaat. Misschien moeten wij ons als Kamer, suggereerde hij, niet al te druk maken over het wel of niet definiëren van de zorg als vitale sector, omdat het de facto als geregeld is. Wat vindt de Minister daarvan?

Minister **Grapperhaus**:
Ik vind het goed dat u zich daar ter plekke met mensen over verstaat en gaat kijken hoe het in zijn werk gaat, want dan kunnen we er met elkaar verdiepend over praten. Ik ben nog niet zover dat ik zeg dat als de mensen van het Z-CERT zeggen dat het wel goed gaat, we er zijn. Ik vind het ook echt – dan kom ik weer even terug op het begin van mijn beantwoording aan mevrouw Buitenweg – dat het betreffende departement op een gegeven moment moet aangeven: dit is toch echt vitaal, hier moeten we die extra zekerheden opzetten. Dat moeten ze motiveren. Ik had – dat geef ik eerlijk toe en dat heb ik ook in die Kamerbehandeling laten blijken in 2018 – best wat second thoughts over of je de zorg er niet toch voor een deel onder zou moeten hebben. Dat was natuurlijk ook ingegeven – u kunt zich dat herinneren – door die twee Engelse ziekenhuizen die in de zomer 2017 met problemen geconfronteerd werden op dit gebied. Ik vind echt dat het Ministerie van VWS grondig moet ingaan op het verzoek dat in de motie van mevrouw Van den Berg besloten ligt. Dat klinkt misschien wat streng naar een collega-departement, maar mijn ministerie – zo heb ik dat steeds ook naar uw Kamer geformuleerd – moet de rol hebben van aanjager op dit punt en de departementen moeten uiteindelijk zelf – zij kunnen dat het beste beoordelen – bepalen: hier is een nadere bepaling nodig, een benoeming als vitale sector, of niet. Het punt dat de heer Verhoeven noemt zal zeker ergens in de Kamerbrief een plek krijgen, over hoe dat met het Z-CERT geregeld is.

De heer **Verhoeven** (D66):
Ik heb tien jaar lang heel veel geleerd van CDA-Kamerleden en -bewindslieden. Een van de lessen die ik van het CDA geleerd heb, is dat je niet het kind met het badwater moet weggooien. Dat is een wijsheid die veel CDA'ers aan mij verteld hebben. Ik zou de Minister dan hier willen vragen om, mocht het nou zover komen dat er besloten wordt om de

zorgsector niet meer via het Z-CERT, maar gewoon direct als onderdeel van de vitale infra te definiëren, de opgebouwde structuur, die al een bepaalde werkingskracht heeft, niet direct weer los te laten. Ik denk dat de Minister dat oordeel deelt, dus misschien hoeft hij daar dan niet heel uitgebreid op in te gaan.

Minister **Grapperhaus**:
Als CDA'er – dat is bekend dacht ik, dat ik van het CDA ben – moet ik zeggen dat ik voor alles wat met het gezin te maken heeft zeer pal sta. Dus inderdaad, ik heb mijn vier kinderen ook grootgebracht zonder het badwater. Ik begrijp dat de heer Verhoeven hier die beeldspraak gebruikt. Hij begrijpt hoop ik ook van mij, al dan niet gezinstechnisch ingevoerd, dat het ministerie moet zeggen – nu is dat Medische Zorg, maar een volgende keer is dat Infrastructuur – of het vitaal is, en om welke redenen, of dat het niet vitaal is.

De **voorzitter**:
Gaat u verder. Hoewel, mevrouw Buitenweg wilde geloof ik nog even doorgaan op haar interruptie.

Mevrouw **Buitenweg** (GroenLinks):
Ik heb één echt heel korte vraag. Wat ik toch nog niet begreep, is of dat «pas toe of leg uit» gaat gelden voor alle vitale sectoren ongeacht of het private of publieke aanbieders zijn.

Minister **Grapperhaus**:
Nou, ja. Wat ik in kaart wil brengen, is wat het huidige wettelijke instrumentarium hierop is en wat een aanvullend instrumentarium zou kunnen zijn om dat «pas toe of leg uit» zo ver mogelijk te laten reiken. Ik vertelde u al dat het natuurlijk een reactie is geweest op het WRR-rapport over cybersecurity, wat zich in één zin laat samenvatten: het is niet de vraag of er iets helemaal misgaat een keer, het is alleen maar de vraag wanneer dat gaat gebeuren. Nog geen drie maanden later hadden we Citrix en het kan natuurlijk nog erger. Ik wil hier ook niet allemaal hoge verwachtingen wekken over dat «pas toe of leg uit», want het moet allemaal wel kunnen. Maar ik vind wel dat we – mevrouw Buitenweg heeft dat als zorg geuit – het niet alleen moeten hebben over puur de overheid of de vitale aanbieders, maar ook zeker over de bedrijven die belangrijke raakvlakken hebben met de overheid. Maar nogmaals, we moeten dat wettelijke instrumentarium wel goed in kaart hebben, want het moet een goede grondslag hebben.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Mevrouw Buitenweg vraagt wat de overheid onderneemt om veilig in te kopen. Dat ligt, zo geef ik toe, enigszins op het terrein van de collega. De Roadmap Digitaal Veilige Hard- en Software van de Staatssecretaris van Economische Zaken en Klimaat geeft een heel samenhangende aanpak op dat punt. We willen ook echt vooroplopen ten aanzien van digitale veiligheid van hard- en software. Die roadmap is overigens een invulling van de Nederlandse Cybersecurity Agenda. Daarin kunt u de uitgangspunten daarvoor terugvinden. Dat moet natuurlijk ook in de hele productontwikkelingscyclus bevorderd worden. Door criteria hiervoor in het inkoopbeleid op te nemen, zul je als aanbieder van de overheid in ieder geval aan die eisen moeten voldoen. Dan kom ik even terug op waar we het net over hadden. Dit zou een van de middelen kunnen zijn om bepaalde partijen een stuk cybersecureder, meer cybersecure, te maken.

Dit is op allerlei manieren uitgewerkt en ik kan het niet nalaten om dit te noemen. Er is ook een zogenoemde wizard Inkoopeisen Cybersecurity Overheid gekomen. Dat is een tool die op dit moment in pilots getest wordt bij overheidsorganisaties uit de vier bestuurslagen: Rijk, provincies, gemeenten en waterschappen. Dat is dus echt een tool waarmee je kunt bekijken waar je aan moet toetsen, zodat je niet het wiel opnieuw hoeft uit te vinden als lokale overheid.

Mevrouw **Buitenweg** (GroenLinks):
Ik ben heel blij met de wizard, maar de vraag was of het klopt dat departementen allemaal apart databeveiligingsproducten inkopen. Ik vraag dat omdat ik denk dat je als je dat meer als geheel doet een stimulans hebt voor bepaalde bedrijven. Dan heb je gelijk ook een grotere afzetmarkt, wat dan weer aansluit bij mijn pleidooi om een aantal bedrijven te stimuleren om van de grond komen. Mijn concrete vraag is dus of het klopt dat departementen apart databeveiligingsproducten inkopen en of de Minister bereid is om te koersen op meer centrale regie daarop.

Minister **Grapperhaus**:
Dat is een gedachte die ik bij mijn collega van Binnenlandse Zaken moet neerleggen, die natuurlijk verantwoordelijk is voor de digitale overheid. De inzet is in ieder geval om die wizard zo breed mogelijk neer te zetten. Dat betekent dat je steeds dezelfde rekenliniaal krijgt, als u een beetje de vergelijking begrijpt, die langs de producten wordt gelegd. Ik zal de gedachte doorspelen op het punt van steeds meer gezamenlijke inkoop, want die begrijp ik en dat wil ik hier best hardop uitspreken. Maar ik moet wel een beetje oppassen. Ik moet me niet als Minister van JenV op het terrein van de rijksinkoop begeven. Laat ik het zo zeggen: ik onderschrijf dat het een goede suggestie is en ik zal haar doorgeleiden van de collega's staatssecretarissen van EZK en BZK, en vooral die laatste.

Mevrouw **Buitenweg** (GroenLinks):
Daar ben ik heel blij om. Wij hebben eerder gepleit voor een centralere aansturing vanuit het kabinet, omdat dit punt precies op het terrein van Binnenlandse Zaken ligt. Als wij onze inkoopmacht gebruiken, kan dat de cyberveiligheid vergroten, waar deze Minister dan weer voor is. Dat is wat anders dan dat het allemaal langs een bepaalde meetlat gaat, want het kunnen heel veel, wel honderd, producten zijn die langs die meetlat gaan. Als je een aantal daarvan echt stimuleert, dan kan dat juist die bedrijven van de grond tillen. Ik ben blij dat de Minister dit gaat doorspelen aan zijn collega's, maar ik zou op een bepaald moment wel geïnformeerd willen worden over of hier wat meer centrale regie op komt. Ik denk echt dat het belangrijk is die inkoopmacht te gebruiken.

Minister **Grapperhaus**:
Ik heb al gezegd dat ik het punt ter harte neem. Maar u moet natuurlijk begrijpen dat... Als het gaat om de centrale inkoop van stroomstoot-wapens, dan voel ik mij ook in het executieve aangesproken. Hier moet ik... Met een positieve advisering of positieve grondhouding – zo noemde premier Lubbers dat vroeger, geloof ik – geef ik dit door aan de collega van BZK.

De **voorzitter**:
Ja, maar de vraag is of de Kamer wordt geïnformeerd over het resultaat daarvan.

Minister **Grapperhaus**:
Nou, laat ik het zo zeggen. Mevrouw Buitenweg heeft wel gelijk dat ik de aanjager moet zijn voor cyberveiligheid. Ik zal zorgen dat we in de brief

over «pas toe of leg uit» ook een klein kopje aan dit onderwerp wijden. Dat is fijn, want dan kan dat ook mede namens de collega. Dat is dan ook weer leuk.

De **voorzitter**:
Dat is altijd mooi. Zo zien we het graag. Gaat u verder.

Minister **Grapperhaus**:
Gezelligheid troef in deze donkere tijden.
Voorzitter. Dan de bescherming van onze gemeenten. Ik vind de digitale veiligheid bij gemeenten echt van heel groot belang. Het is echt zorgelijk dat een gemeente, Hof van Twente, getroffen is door een hack. Er is meteen contact geweest vanuit mijn ministerie, het NCSC, met de collega van Binnenlandse Zaken. Ik heb van de collega vernomen dat de IBD... Dat is in dit geval het CERT voor de gemeenten, het Cyber Emergency Response Team. De heer Verhoeven noemde die afkorting net al, maar ik doe het nog even voor de mensen die meekijken. In ieder geval heb ik begrepen dat de IBD in contact staat met de gemeente om hulp te verlenen en dat men zo goed mogelijk en zo snel mogelijk de problemen daar wil oplossen. Ook daar heb ik in ieder geval heel duidelijk het dringende advies gegeven – althans, dat hebben mijn mensen gedaan – dat je bij ransomware weg moet blijven bij betalingen of het toegeven aan eisen. Ik neem aan dat dit in het AO Digitalisering van morgen met de collega van BZK uitvoeriger aan de orde zal kunnen komen. Dat wil ik nu niet in de weg lopen.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Dank voor deze toelichting, maar de vraag aan de Minister was of er een helder protocol en een crisisplan zijn. Zo niet, wordt daar nu aan gewerkt naar aanleiding van Hof van Twente maar ook andere voorbeelden?

Minister **Grapperhaus**:
Bij de gemeente, bedoelt u? De collega van BZK is hier degene die aan slag is. Morgen bij het AO Digitalisering zullen alle vragen hierover ten aanzien van deze gemeente aan de orde komen. Voor ons geldt heel duidelijk dat er vanuit het NCSC richting een partij die in de problemen is heel duidelijke protocollen gevolgd worden. Maar u bedoelt... Pardon, uw lid Yeşilgöz bedoelt te zeggen: hoe zit dat bij die gemeente? Daarvoor wil ik echt verwijzen naar dat AO, ook omdat – dat geef ik eerlijk toe – ik feitelijk niet precies weet hoe daar de stand van zaken is.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Ik begrijp dat die verantwoordelijkheden óf elders liggen of in het midden liggen. Maar als een gemeente bijvoorbeeld te laat een signaal afgeeft dat zoiets gaande is – zo is het bij Hof van Twente gegaan – en men te lang wacht, dan zitten die criminelen al in die systemen. Ik zie hier ook een verantwoordelijkheid voor de Minister van JenV. Ik vind het prima om mijn collega's mee te geven om die vragen morgen daar te stellen, maar volgens mij is er hier wel een gezamenlijke verantwoordelijkheid. Hoe voorkom je dat criminelen te lang in systemen kunnen blijven zitten? Ik snap dat gemeenten snel kunnen signaleren en dan opschalen via een protocol van BZK, maar er is hier ook een rol voor JenV.

Minister **Grapperhaus**:
Het zal mevrouw Yeşilgöz misschien verrassen, maar ik ben op zichzelf wel blij dat zij dit zegt. Dat verheugt mij, want ik denk dat het heel erg van belang is dat het NCSC en het CERT, het Cyber Emergency Response Team dat daarbinnen werkt, er onmiddellijk bij betrokken worden. Dat moet in het dna zitten van iedereen bij elke gemeente. Als die er niet uitkomen, dan moet onmiddellijk ook het NCSC het erbij betrokken

worden. Daar moeten we echt met elkaar naartoe. Ik ga niet een oordeel uitspreken over hoe het hier precies gelopen is. U kent mijn vaste mantra: over individuele zaken doe ik geen uitspraak. Maar goed, hier is dus ook morgen een AO over. Maar ik onderschrijf wel dat het zo zou moeten zijn. Nu is alleen het punt dat we met elkaar wel moeten vaststellen – daar kom ik in de brief van begin volgend jaar ook nog op terug – tot hoever het wettelijk instrumentarium nu eigenlijk strekt. Ik zeg heel eerlijk dat we daar met elkaar echt nog wat slagen te maken hebben.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Mevrouw Yeşilgöz vroeg hoe het staat met de motie van mevrouw Laan en de heer Verhoeven over kwetsbaarheden. Ik kan u meedelen dat er een onderzoek is uitgevoerd bij de departementen naar het geautomatiseerd zoeken naar kwetsbaarheden. Daaruit blijkt dat het breed wordt toegepast. Er is ook behoefte aan kennisdeling. In de kabinetsreactie op het WRR-rapport is ook toegezegd dat de CIO Rijk in afstemming met NCTV, NCSC en de departementen een handreiking opstelt voor het scannen. Die is as we speak, ongeveer eind dit jaar in concept gereed. Via het informatiebeveiligingsbeleid wordt getoetst of de rijksorganisaties daar invulling aan geven. Op dit moment ligt de focus ook op externe scanning. Er wordt tooling aangeschaft voor het uitvoeren van externe scans, de zogenaamde Shadow Tracker, zodat partijen die daarover nog niet beschikken ook de stappen kunnen maken. Dit moet helemaal worden uitgerold, zeker zodra we de handreiking helemaal hebben goedgekeurd.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Om een tweede termijn te voorkomen en ook – als ik heel eerlijk ben – om de antwoorden te snappen, vraag ik of nou goed begrijp dat er nu handreikingen worden geformuleerd voor een scan, maar dat die scans nog niet hebben plaatsgevonden. Want dat was mijn vraag: is er een scan geweest van de vitale infrastructuur? Begrijp ik dat de Minister zegt: dat zijn we nu aan het opzetten? En als ik dat goed heb begrepen, is mijn vraag: wanneer is die scan dan?

Minister **Grapperhaus**:
Het wordt al breed toegepast, maar of dat zo consistent wordt gedaan dat het helemaal in die handreiking past, zal de komende tijd moeten blijken. Die handreiking is er nu. Er was al sprake van het geautomatiseerd zoeken naar kwetsbaarheden, want dat is onderzocht. Maar zodra die handreiking er is, moeten we gaan kijken of wat er nu gebeurt ook helemaal in overeenstemming daarmee is en of dat ook echt up to standard is. Daar doe ik nu even geen uitspraken over.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Ik hoor dus: nee, er wordt nog niet structureel gescand. Ik ga nu even invullen dat dat komend jaar wel gaat gebeuren, maar daar komen we dan op terug. Dat is een. Twee. Om even terug te komen op het debat dat er net was over crosssectorale oefenprogramma's: ik begreep – ik vraag dit wederom om het goed te begrijpen – dat de Minister zegt dat er voor komend jaar zomer een oefenprogramma uitgerold zal worden. Heb ik dat goed begrepen? Betekent het dat dit daarmee structureel wordt opgezet? Want dat was een van mijn vragen. Het wordt dus voor die zomer en daarna structureel? En zijn de vitale bedrijven daarbij ook aangehaakt? Is het dus vormgegeven zoals in de motie werd gevraagd: met de vitale bedrijven en structureel?

Minister **Grapperhaus**:

Volgens mij is dat – maar ik ga niet die hele tekst er weer bij halen – helemaal op die manier uitgevoerd. Ja. Het is goed om daar geen misverstand over te hebben nu we bij elkaar zitten. U begrijpt: dat gaat per departement. Per departement was men, zo is vastgesteld, al aan de slag met het geautomatiseerd zoeken naar kwetsbaarheden. Maar naar aanleiding van het WRR-rapport heeft de CIO gezegd: oké, ik maak daar nog eens een hele handreiking voor. Ik heb er goed vertrouwen in dat dat bij een aantal departementen al helemaal conform de handreiking gaat. Het zal misschien bij een aantal niet helemaal zo gaan; die moeten alsnog up to standard worden.

De **voorzitter**:
Mevrouw Yeşilgöz, kort.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Ja, maar ik begin het wel te begrijpen, dus dat scheelt, voorzitter. Wie gaat erover? Want zo'n handreiking is vrijblijvend. We hopen dat iedereen die vervolgens opvolgt. Wie coördineert dat vervolgens? Wie houdt daar toezicht op? Of mogen we daar dan straks de Minister, die nu naar mij lacht, op aanspreken?

Minister **Grapperhaus**:
Ik heb in die drie jaar en twee maanden geleerd dat ik op alles kan worden aangesproken, maar dit ligt primair bij de CIO Rijk. Dat is degene die de digitale overheid aanstuurt; dat heb ik eerder uiteengezet, maar dat is ook algemeen bekend, dacht ik. Maar NCTV en vooral NCSC hebben daarin een aanjagende rol; dat heb ik ook eerder gezegd. U mag mij dus op het laatste aanspreken: voldoet het NCSC wel aan zijn aanjagende rol? Maar de Staatssecretaris van Binnenlandse Zaken moet naar u toe verantwoording afleggen over of de CIO Rijk dat doet. Wij werken daarin samen. Ik zie een enkeling een beetje geprangd kijken, maar het is zo dat...

De **voorzitter**:
Nee, hoor.

Minister **Grapperhaus**:
Misschien had ik het over de overvolle publieke tribune. Maar ik wil het allemaal graag uitleggen. Met de twee collega-staatssecretarissen van EZK en BZK overleg ik zeer regelmatig om ervoor te zorgen dat de rolverdeling tussen ons goed blijft lopen, ook in Europees verband als het gaat over dingen als Internet of Things.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Dan was er de kwestie, ook van mevrouw Yeşilgöz, over het mkb. Er is het Digital Trust Center, dat zich nadrukkelijk richt op het niet-vitale bedrijfsleven, waar het mkb een belangrijk onderdeel van is. Het werkt samen met het NCSC om informatie te ontsluiten in informatiekennisproducten, zoals bijvoorbeeld de cybersecurity-risicoscan voor bedrijven. Men werkt aan het vertalen van dat soort vaak hoogwaardig-technische informatie naar een concreet handelingsperspectief, als ik het zo mag noemen, met een soort gebruiksaanwijzing zodat het ook echt hanteerbaar is voor mkb-bedrijven. Er is bijvoorbeeld een website met onder andere de vijf basisprincipes voor veilig digitaal ondernemen. Er is een platform waar partijen elkaar met best practices of juist worst practices kunnen helpen. Voorzitter. Dan de vraag over hatespeech, even een iets ander onderwerp. Laat heel duidelijk zijn dat alle vormen van discriminatie onaanvaardbaar zijn. Hatespeech valt daar ook onder. Uitgangspunt van het beleid is dat

online dezelfde regels gelden als offline. Dat betekent dat de aanpak online door de omvang en de betrokkenheid van providers en platforms een aantal extra uitdagingen kent. Een deel van de verantwoordelijkheid om hatespeech tegen te gaan ligt wat het kabinet betreft bij platforms en providers. Ook verschillende meldpunten en de politie zelf spelen een cruciale rol bij het vaststellen of er sprake is van hatespeech. De notice-and-take-downprocedures die we hebben en die we ook vanuit de EU kennen, zijn erop gericht om onrechtmatige en strafbare uitingen verwijderd te krijgen. We hebben dat onlangs in een aantal gevallen gezien. Ik noem de journaliste die door een aantal mensen bedreigd en lastiggevallen werd en hatespeech over zich heen kreeg. Ik noem ook de opsporing in het kader van de bedreiging van een leraar in Rotterdam onlangs. Ik kan nog meer voorbeelden noemen, maar ik zal me nu even hiertoe beperken. Als er een dader bekend is, dan komt er zo snel mogelijk Europese opvolging. In Europees verband – ik kom daar zo ook op terug bij andere dingen zoals kindermisbruik – steunt het kabinet de ambitie om de strijd tegen online haatzaaiende uitlatingen op te voeren. Je hebt natuurlijk het beroemde evenwicht – daar hoef ik niet veel over uit te leggen – tussen het recht op vrijheid van meningsuiting en de illegale online inhoud van internetuitlatingen. Dat is een delicaat evenwicht; laat ik het zo zeggen.

Voorzitter. Over de statelijke actoren kan ik in ieder geval zeggen dat ik in de eerste maanden van het volgend jaar met een brief kom. Als ik zeg «volgend jaar», dan is dat natuurlijk wat diffuus in het licht van de verkiezingen, maar ik wil met een brief komen voordat die zijn geweest. Het is natuurlijk duidelijk dat statelijke actoren digitale middelen inzetten. Daar hebben we vaak in het openbaar over gecommuniceerd. U ziet het ook terug in het Cybersecuritybeeld Nederland. Spionage en sabotage vormen een groot digitaal risico voor Nederland. Het verhogen van de digitale weerbaarheid is daarom echt van het grootste belang. Daarvoor zetten we ons in binnen de aanpak van statelijke dreigingen. Ik geef daar toch even ietwat meer over aan richting mevrouw Yeşilgöz, want anders wordt het een wel heel procesmatig antwoord: volgend jaar krijgt u een brief. We investeren in de operationele diensten om die dreigingen te voorkomen en om de diensten adequaat op een incident te kunnen laten reageren, bijvoorbeeld via de Wet beveiliging netwerk- en informatiesystemen. Die wet heet heel herkenbaar voor iedereen de «cybersecuritywet», maar er is toen een initiatief gekomen om hem de «Wet beveiliging netwerk- en informatiesystemen te noemen», wat op zichzelf ook een mooie benaming is.

Voorzitter. Dan nog even dit. Ik ben ermee bezig opvolging te geven aan de motie die mevrouw Buitenweg bij de begrotingsbehandeling heeft ingediend, omdat zowel de dreiging als de technologie zich zeer snel ontwikkelt. Dat zien we natuurlijk aan allebei de kanten. De aanpak moeten we voortdurend aanpassen aan hoe de ontwikkelingen ervoor staan. Wat ik eigenlijk wil gaan doen, is de structurele samenwerking die we voor het eerst binnen de 5G-aanpak hebben gebruikt en waaruit ook de taskforce is voortgekomen, uitrollen naar andere vitale processen. Want dan hebben we in die vitale processen dus precies een soortgelijke benadering, van wie onze leveranciers worden, hoe onze systemen eruit gaan zien enzovoorts.

Voorzitter. Als u dat goed vindt, ga ik nog even in op het protocol voor ransomware. Via u wil ik in ieder geval aan mevrouw Yeşilgöz melden dat de VNG dit jaar een drietal cyberoefenpakketten heeft ontwikkeld, die zij gratis ter beschikking heeft gesteld aan alle gemeenten. Zo kan men op het terrein van cybercrisismanagement in ieder geval voor zichzelf een handelingsperspectief ontwikkelen en daarmee oefenen. Dat is een onderdeel van ervoor zorgen dat er duidelijke handelingslijnen zijn.

Voorzitter. Dan kom ik op de vragen van het lid Van Dam. Laat ik vooropstellen dat ik het idee van een soort digitaal weerbericht heel interessant

vind. Ik zeg daar even bij dat er op dit moment al verschillende mogelijkheden zijn die daaraan raken. Er zijn allerlei informatiepunten, variërend van www.veiliginternetten.nl tot informatiepunten waar allerlei uitleg wordt gegeven over onlineveiligheid en dergelijke. Ook is er het aanspreekpunt Slachtofferhulp Nederland voor als je echt slachtoffer bent geworden. Ik vind het een interessante gedachte om te kijken of je iets zou kunnen doen. Ik zeg het even spontaan: ik ben wat voorzichtig met zeggen dat mensen dat dan op hun computer binnenkrijgen, want voor je het weet wordt daar ook weer via «fishingweerberichten» – als u het woord een beetje begrijpt – misbruik van gemaakt. Maar ik vind het wel interessant om te kijken of je het publiek en het bedrijfsleven gestructureerder kunt waarschuwen voor bepaalde zaken. Ik wil wel even het volgende zeggen, want dat hebben we bij Citrix gezien. Als het echt om een heel erg macro aanwezig programma gaat en het Nationaal Cyber Security Centrum, het NCSC, geeft waarschuwingen – die hebben bij Citrix tot het zogenaamde HIGH/HIGH-waarschuwingsniveau geleid – dan zijn er toch nog partijen die zich daar niet aan houden. Maar je zou je wel kunnen afvragen of het mogelijk is om dat in bredere zin op te zetten, op een centraal punt, zodat mensen daar in ieder geval goed kennis van kunnen nemen. Dus ik ga dat onderzoeken en ik kom daarop terug in een brief.

De heer **Van Dam** (CDA):
Fijn. Ik krijg bijvoorbeeld iedere zondagavond zelf van een meneer de nieuwsbrief van Cybercrimeinfo. Zo zijn er allemaal dingen. Je hebt ook een Facebookpagina over hoaxes, waar je ook kunt zien wat er allemaal speelt. Ik wil helemaal niet zeggen dat het ministerie dit moet gaan doen, maar ik zou mij kunnen voorstellen dat bijvoorbeeld een omroep hierin geïnteresseerd is en dit wil doen. Ik dank de Minister voor het bekijken daarvan. Wat mij betreft, moet het inderdaad iets zijn wat mensen niet online, maar op een andere manier lezen. Het moet voor iedere burger gewoon een meer normaal onderwerp worden, zodat we die awareness omhoog krijgen. Dat is een beetje het idee erachter. Maar vol verwachting klopt mijn hart, ook al is Sinterklaas het land alweer uit.

Minister **Grapperhaus**:
Overigens: door de snelheid van de stoomboot is hij nog ergens in de buurt van de Golf van Biskaje. Maar dit geheel terzijde.

De **voorzitter**:
Windje mee.

Minister **Grapperhaus**:
Ja! Voorzitter. Ik kom er in een brief op terug, want de heer Van Dam zegt meteen dat dit niet online hoeft, maar dat weet ik niet. Laat mij erop terugkomen. Ik vind het namelijk een interessant idee, en daar blijf ik op dit moment maar even bij.

De **voorzitter**:
Mevrouw Yeşilgöz heeft daar ook nog een vraag over.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Een weerbericht: het is allemaal prima dat we dat gaan uitzoeken. Ik hoorde de Minister zeggen dat ook ondernemers die informatie willen. Dat is de reden waarom ik vroeg naar het Digital Trust Center en de landelijke dekking. Als we die op orde zouden hebben, dan zouden de ondernemers op tijd gewaarschuwd kunnen worden als er iets gaande is. Mkb'ers hebben daar heel vaak aandacht voor gevraagd. Ik hoor de Minister daar in zijn antwoorden eigenlijk niet echt uitgebreid op ingaan. Ja, ik hoor een herhaling van de dingen die ik ook heb gelezen, maar ik wil

gewoon weten wat de verklaring is voor het achterblijven van dat landelijk dekkend stelsel. Ik vind het prima als dat in de brief terugkomt, die we dan hopelijk snel krijgen. Maar er is dus eigenlijk al een manier om in ieder geval mkb'ers op tijd te waarschuwen – dat is iets anders dan een weerbericht – en te zeggen dat er een storm aan komt. Dat kan, maar dat gebeurt nog niet.

Minister **Grapperhaus**:
Mevrouw Yeşilgöz heeft terecht gewezen op het landelijk dekkend stelsel. Dat is in opbouw. We zetten erop in, die landelijke dekking ook te krijgen door middel van het opzetten van samenwerkingsverbanden. Maar ja, daar hebben we de sectoren zelf natuurlijk ook bij nodig. Daar ziet u een beetje het punt waarover ik eerder met mevrouw Buitenweg even van gedachten wisselde. We moeten wel kijken tot hoever het instrumentarium gaat waarbij je kunt verplichten om mee te doen of waarin je in ieder geval een zodanige prikkel in kunt bouwen dat men meedoet. Maar daar zetten we op in. In de voortgangsrapportage over de NCSA van volgend jaar, de agenda van het Nationaal Cyber Security Centrum, zullen wij daarover verder rapporteren. Dan kunnen we kijken hoever we zijn en waar het nog aan dekking ontbreekt. Als we dan echt zien dat er dan nog – hoe noem je zoiets? – blinde vlekken op de kaart zijn, dan zullen we, denk ik, vooral met u van gedachten moeten wisselen over hoe we dat gaan oplossen. Dat zit «m er dan echt wel in dat sommige sectoren of delen van sectoren die samenwerking om wat voor reden dan ook een beetje afhouden; dat zeg ik heel eerlijk. Er komt zelfs al eerder een brief over het landelijk dekkend stelsel, namelijk begin volgend jaar. Dan kan ik dus zelfs nog beter nieuws hebben. Die komt ergens in januari-februari 2021. Laten we prikken op uiterlijk de dag voor ingang van het reces.

De **voorzitter**:
Welk reces?

Minister **Grapperhaus**:
Dat is een goede, maar ik dacht het eerste reces in 2021. En dan tel ik het tweede deel van het dan lopende kerstreces niet mee.

De **voorzitter**:
Laten we daar ook een aparte brief aan wijden. Welk reces? Niet 4 januari. Dat begrijp ik in ieder geval wel.

Minister **Grapperhaus**:
Nee.

De **voorzitter**:
Het krokusreces.

Minister **Grapperhaus**:
Dan ben ik -80°C-dingen aan het doen, heb ik begrepen.
Voorzitter. De HashCheckService is nog aan de orde gesteld door de heer Van Dam. Inderdaad, in de database staan bij de HashCheckService hashes van strafbaar kinderpornografisch beeldmateriaal. Dat zijn dus digitale vingerafdrukken. Die worden vergeleken met de unieke digitale vingerafdrukken van het beeldmateriaal bij een bepaalde service, en als er een match is, dan kun je er dat meteen vanaf halen. Dan hoef je dat materiaal verder niet te openen en te bekijken. Het klinkt allemaal heel triest, maar dat geeft een enorme efficiencyslag, gezien de duizelingwekkende hoeveelheden waar we het over hebben. Dan kan het materiaal ook worden verwijderd en dan wordt het internet schoongemaakt en ontdaan van die rotzooi. Want het feit dat dit heel vaak opnieuw opduikt is, terecht, een van de verdrietigste dingen voor slachtoffers van kinderporno. Op dit

moment wordt de HashCheckService uitgebreid met het zogenoemde Photo-DNA.
Hoe zit het met de Europese Unie? Ik zal het kort zeggen. Pardon?

Mevrouw **Buitenweg** (GroenLinks):
Het klonk als een open vraag: hoe zit het met de Europese Unie? Vandaag is dat op de Europese top een belangwekkende vraag.

De **voorzitter**:
Kunnen we daar ook een «weerbericht» over beginnen: Hoe is het vandaag met de Europese Unie?» Gaat u verder, Minister.

Minister **Grapperhaus**:
Voorzitter. Ik vind het in ieder geval plezierig dat we dit kritische debat in zo'n goedgeluimde sfeer voeren. Waarom niet? Nou, dat komt waarschijnlijk doordat we zo'n waardeloze voorzitter hebben...
Voorzitter. Dit is even een belangrijk punt. Ik heb het wel eerder gezegd in AO's en ik heb het ook geschreven: op mijn aanvankelijke verzoek om steun in het voorjaar van 2019, aan de vorige Eurocommissaris, heb ik volledig bot gevangen. Hij was niet geïnteresseerd. Ik ga het even heel hard zeggen: de nieuwe Eurocommissaris, mevrouw Ylva Johansson, is echt zeer dedicated op dit punt. In oktober 2019 heb ik in Luxemburg tijdens een informele ministerraad een vrij stevig punt ingebracht tegen de toen aanwezige grote techbedrijven. Ik heb ook het verwijt gemaakt dat op de agenda tweeënhalf uur tijd was vrijgemaakt voor terrorisme online en een kwartier voor kinderporno. Ik moet mevrouw Johansson echt een compliment maken op dit punt. De ernst en de verschrikkelijke hoeveelheden: dat mag echt nog een keer gezegd worden. Het neemt werkelijk wanstaltige vormen aan en het staat ook gewoon – voor degenen die thuis zitten te kijken – op Instagram. Op dat soort hele brave huiselijke sociale media kun je de meest verschrikkelijke beeldmaterialen en dergelijke uitwisselen. Nou, er is een actieplan van de Europese Commissie. Dat is op 25 september in een BNC-fiche aan uw Kamer gestuurd. Daarin heb ik ook steun gegeven aan dingen waar de Europese Commissie nu mee komt. Men heeft een achttal initiatieven; ik noem: preventie, passende hulp voor slachtoffers, vervolging van misbruik en dat effectieve onderzoek. Men heeft ook heel veel interesse voor de HashCheckService die we hebben – daarover zijn we in gesprek – en voor de bestuurlijke aanpak. Daarover heb ik uw Kamer een paar weken geleden gemeld dat BZK en wij het erover eens zijn dat daarvoor een zbo zal komen.
Wat zijn de resultaten van die HashCheckService? U heeft gezien dat ik een waarschuwingsbrief heb gestuurd naar de hostingproviders. Het grootste deel van hen heeft allerlei maatregelen getroffen, ook preventieve maatregelen, om te voorkomen dat hun servers na een schoonmaakactie opnieuw zouden worden vervuild. Twee bedrijven kwamen er in het rapport van de TU Delft heel slecht uit. Die waren daarover not amused, maar ja, het was nou eenmaal aangekondigd dat het rapport bekendgemaakt zou worden. Je kunt zeggen dat het goed nieuws is, maar het is ook heel slecht nieuws: door de toename van het gebruik van de HashCheckService zijn nu al – u gelooft mij niet – 18,2 miljard afbeeldingen gecheckt en 7,4 miljoen afbeeldingen van online seksueel kindermisbruik gedetecteerd. 7,4 miljoen! De HashCheckService is dus echt een enorm succes, maar we mogen wel vaststellen dat er een ongelofelijke hoeveelheid vuiligheid op internet staat. Ik zet het gewoon allemaal maar eens neer, want dit onderwerp verdwijnt iedere keer naar pagina 34 van de krant.
Voorzitter. Is het verstandig...

De **voorzitter**:
Een ogenblik. Meneer Van Dam.

De heer **Van Dam** (CDA):
Ik weet niet of de Minister klaar is met het onderwerp kinderporno. Ja. Ik had een vraag gesteld over die HashCheckService. Het is een prachtig instrument – laten we dat vooropstellen – maar hij is vrij kwetsbaar, want als je een klein dingetje verandert aan je afbeelding, dan kun je weer vrolijk verder. Is daarin voorzien? Dan een tweede vraag. De Minister zegt dat er vanuit Europa dingen gebeuren. De brief over internetcriminaliteit en Naar een veiliger samenleving is van 20 mei. Dat is een beetje het nadeel als het lang duurt voordat een AO plaatsvindt. Daarin lees ik vooral iets over de Nederlandse aanpak van kinderporno. Is de beweging die de Minister beschrijft van na 20 mei? Is die recent? Het zou mij namelijk heel erg geruststellen als kinderporno in Europees verband wordt aangepakt, als iedereen zijn deskundigheid op de mat legt en als we daar samen dingen in doen.

Minister **Grapperhaus**:
Ja. Ik kom meteen even op dat laatste. Op dat eerste punt kan ik niet direct antwoorden. Ik kom bij u in januari in een brief terug op de vraag of die HashCheckService eenvoudig te manipuleren is. Wat het tweede punt betreft dat u noemt: er is na 20 mei 2020 inderdaad veel gebeurd. Voor mei 2020 had mevrouw Johansson mij al in persoonlijke gesprekken gezegd dat zij hier een speerpunt van ging maken. Overigens had de vorige Commissaris van Justitie, mevrouw Jourová, dat ook al een beetje aangegeven. Maar goed, zij is daar heel erg mee bezig. Ik dacht dat ik in een brief in het najaar hieraan gerefereerd had, maar ik constateer dat dat niet zo is, dus ik zeg toe dat ik in januari in de brief waarin ik inga op de HashCheckService, ook precies aangeef waar wij in Europees verband staan.

De heer **Van Dam** (CDA):
Heel graag. Wat mij betreft kan het om de dingen wat bij elkaar te houden ook in een brief met allerlei dingen die misschien uit dit AO voortvloeien, maar dat laat ik graag aan de Minister over.

De **voorzitter**:
Dank u wel. Ook mevrouw Buitenweg heeft hier een vraag over.

Mevrouw **Buitenweg** (GroenLinks):
Nou ja, eigenlijk over Europa en wat er allemaal in Europees verband wordt gedaan of niet. Ik begrijp dat het Europees Medicijnagentschap, EMA, ook doelwit is geworden van een cyberaanval. Ik zie dat de Nederlandse autoriteiten mede onderzoek doen. Wordt samen afgesproken welke eisen er worden gesteld? Is er een Europese afspraak over hoe we omgaan met ransomware? Met name dat laatste wil ik weten.

Minister **Grapperhaus**:
Volgende week wordt de nieuwe EU-cybersecuritystrategie verwacht. Daarover zal ik u zo snel mogelijk door middel van een BNC-fiche adviseren, want samenwerking in EU-verband is hier heel erg belangrijk. Een van u heeft er in eerdere AO's al op gewezen: wij hebben met grootheden te maken in algemene zin als het gaat om het internet, het darkweb en dat soort zaken, maar ook in de zin van grote techbedrijven. Daarom is samenwerking hier echt wezenlijk. Dus ik wil u toezeggen dat wij snel met elkaar in gesprek gaan over die nieuwe EU-cybersecuritystrategie zodra die er is.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Dan de vraag van de heer Van Dam of het verstandig is om vitale systemen over te dragen aan private partijen. Ik onderschrijf dat je heel erg zorgvuldig om moet gaan met dit soort gevoelige systemen en goed moet kijken bij wie dat in handen komt, maar een groot deel van onze vitale processen is in beheer bij private aanbieders. Daar staat tegenover dat er allerlei waarborgen gelden voor de systemen die ze gebruiken. Er is op dit moment geen besluit aan de orde over het overdragen van die systemen. Als dat wel zo is, dan zal ik uw Kamer daar voorgaand over inlichten.

De heer **Van Dam** (CDA):
Ik heb het idee dat ik aan mijn zesde termijn toe ben, voorzitter, maar als u het goed vindt, dan vind ik... Maar goed.
In het rapport van de Algemene Rekenkamer staat toch echt dat dit systeem op termijn overgaat. Ik ben het er helemaal mee eens dat dingen als water, elektriciteit en zorg private in handen zijn, maar hier gaat het om data waarmee bepaald wordt of iemand wel of niet toegang tot Nederland heeft. Ik denk dat data of je een paspoort, een visum of dat soort dingen hebt, publieke data zijn. Ik kan ik me, zeker als ik de Minister naar zijn papieren zie kijken, goed voorstellen dat hij denkt: wat moet ik hier nou weer op antwoorden? Ik zit echt niet te zeuren over dingen die in particuliere handen zijn. Dat is zo. Ik zou hier absoluut niet een soort Rusland of een soort communistisch land willen bouwen waar alles in overheidshanden is. Dat is niet het idee, maar dit is echt andersoortige informatie. Als de Minister toch die brief schrijft, zou hij daar dan ook nog eens een regel aan willen wijden?

Minister **Grapperhaus**:
Dat wil ik zeker. Wij hoeven helemaal niet in de Sovjet-Unie zoals die vroeger was te belanden, maar wij moeten ons realiseren dat de digitale wereld ongelofelijk veel analoge verbindingen volledig overboord heeft gegooid. Dat betekent dat wij bijvoorbeeld heel anders moeten aankijken tegen de systemen die op Schiphol worden gebruikt. 30 jaar geleden, voordat internet was wat het nu is, waren die systemen veel minder verbonden. Ik geef onmiddellijk toe dat wij daar op enig moment met elkaar besluiten over moeten gaan nemen. Daar wijst Algemene Rekenkamer op. Ik zeg toe dat ik in ieder geval in de brief aandacht zal besteden aan dit punt. Die brief zal komen als follow-up op het rapport van de Algemene Rekenkamer.

De heer **Van Dam** (CDA):
Nog één ding, ook om de interesse van de heer Verhoeven voor dit onderwerp op te wekken: het gaat om PNR-gegevens en allerlei gegevens die bij elkaar komen – zo heb ik dat systeem begrepen – die met elkaar leiden tot afwegingen voor douaniers, bijvoorbeeld of iemand wel of niet het land in kan. Daar sloeg ik op aan. Dan denk ik ook een beetje aan cybersecurity by design om te voorkomen dat je daar als overheid toezicht op kan houden. Dat verwonderde mij, maar dank voor de strofen die daar in de brief aan gewijd gaan worden.

De **voorzitter**:
Gaat u verder.

Minister **Grapperhaus**:
Voorzitter. Dan de digitale afhankelijkheid in verband met corona. We hebben op dit moment nog geen extra afspraken gemaakt met providers. Er gebeurt in dit verband wel heel veel via allerlei bestaande afspraken. Er wordt continu veel gedeeld over de kwetsbaarheden en bedreigingen, want wij zijn sinds half maart van dit jaar duizelingwekkend veel meer via

digitale communicatie gaan doen. Dat betekent dat iedereen – ik kan het niet vaak genoeg zeggen – zijn updates tijdig moet installeren en ervoor moet waken dat hij ook al het andere goed beveiligd heeft.
Ik kom op de vragen van het lid Verhoeven. Laat ik beginnen met het deltaplan voor cyber. Ik vind het absoluut mijn taak als coördinerend bewindspersoon om de andere departementen aan te sporen en te adviseren. Het uitgangspunt van dit kabinet is steeds geweest en blijft dat digitale veiligheid in elk domein geborgd moet zijn, maar ook een centraal onderdeel moet worden van de reguliere beveiligingsstructuur. Dat betekent dat ieder departement vanuit zijn eigen verantwoordelijkheid daarmee aan de slag moet gaan. Ik heb in mijn ijver van die aanjaagfunctie ook weleens de waarschuwing gekregen: wacht, de betreffende delen van de rijksoverheid moeten hier echt hun eigen verantwoordelijkheid in nemen. Dat is een heel belangrijk onderwerp, want dat betekent dat ieder departement, ieder deel van de rijksoverheid, met zijn eigen, zoals de heer Verhoeven zegt, deltaplan zou moeten komen. Voor het overige wijs ik nog steeds op onze periodieke Cybersecurity Agenda, die telkens de vervolgstappen verder uitwerkt die genomen moeten worden om cybersecurity op alle niveaus te verwezenlijken.
Voorzitter. De onderhandelingen in de EU over de minimumeisen voor «Internet of Things»-devices. Collega Keijzer van EZK maakt zich in de EU al een aantal jaren sterk voor het stellen van wettelijke minimumdigitaleveiligheidseisen aan apparaten die via de zogenaamde Radio Equipment Directive werkzaam zijn. Daarmee zouden op termijn onveilige apparaten van de markt gehaald kunnen worden. De eisen zullen naar verwachting in het voorjaar 2021 van kracht worden. Dan zal er nog wel een overgangstermijn starten voor marktpartijen. Dit alles is onderdeel van de Roadmap Digitaal Veilige Hard- en Software van het Ministerie van EZK. Verder verwijs ik naar een eventueel debat of AO daarover met EZK. Ik hoop dat de heer Verhoeven daar begrip voor heeft. Ik heb u een onderzoek toegezegd naar de investeringen in cybersecurity. Dat wordt op dit moment uitgevoerd door de Cyber Security Raad. De oplevering wordt verwacht in februari 2021. Ik ga enorm mijn best doen om ervoor te zorgen dat dat er ook op dat tijdstip is, want het zou aardig zijn als ik dat via uw Kamer aan het lid Verhoeven zou kunnen toesturen voor begin maart 2021.
Er was een vraag over de uitbreiding van de bevoegdheden van het NCSC. Dat ligt een beetje in het verlengde van wat ik net al zei over de rol die departementen zelf hebben. Het NCSC is heel erg van belang voor Rijk en vitaal, omdat dat er moet zijn bij uitval of verlies van de integriteit van digitale systemen bij die organisaties, omdat er dan juist een grote maatschappelijke impact kan zijn. Het NCSC heeft al diverse taken om organisaties binnen Rijk en vitaal te ondersteunen bij hun digitale weerbaarheid, zoals het informeren, het verlenen van bijstand en het verrichten van analyses en technisch onderzoek ten behoeve daarvan. Voor niet-vitale bedrijven is er dat Digital Trust Center. Ik heb net in antwoord op mevrouw Yeşilgöz en mevrouw Buitenweg gezegd dat wij werken aan de verdere uitrol om dat landelijk dekkend te krijgen. Verder moeten wij met elkaar de ontwikkelingen enorm goed bijhouden. Ik verricht een verkenning naar de wettelijke bevoegdheden en het cybersecuritystelsel. Daar kom ik begin volgend jaar bij u op terug. Ik heb net toegezegd dat dat komt voor het februarireces van 2021.
Voorzitter, dan dacht ik dat ik alles had gehad van de heer Verhoeven. Hij had nog een vraag over het e-woord.

De heer **Verhoeven** (D66):
Als de Minister daar eerst over begint, had ik daarna nog één ander openstaand punt. Naast encryptie had ik ook nog iets gevraagd over de Europese veiligheidsstrategie, maar daar heeft u al heel veel over gezegd

toen u het had over de Europese cybersecuritystrategie, dus misschien is dat al beantwoord.

Minister **Grapperhaus**:
Zal ik eerst iets over het e-woord zeggen? De heer Verhoeven en ik gaan al een tijdje met elkaar mee en weten dat we met het e-woord encryptie benoemen. Encryptie moet er altijd zijn en blijven. Dat is van groot belang voor de veiligheid van de maatschappij, het bedrijfsleven en de overheid, maar ook van de digitaal levende burger. Het is van belang voor het beschermen van fundamentele rechten en het vertrouwen van de maatschappij in digitalisering. Het mag ook weleens gezegd worden – en dan kijk ik via u even naar de heer Verhoeven – het mag ook weleens uit mijn mond gezegd worden dat dat een heel groot belang is. De inzet en ontwikkeling van hoogwaardige encryptie blijven wat mij betreft hoog op de agenda, maar het effect van encryptie op de effectiviteit van opsporings- en veiligheidsdiensten kan niet worden genegeerd. Wij moeten met elkaar zoeken naar adequate – let goed op dat woord – evenwichtige en technische oplossingen voor de opsporing en de veiligheid die hoogwaardige encryptie voor burgers en bedrijven van goede wil respecteren. De heer Verhoeven kent mij goed genoeg om te weten dat ik mij daar echt voor inzet. We praten hierover in EU-verband. Daarbij is het uitgangspunt dat je moet zoeken naar technische oplossingen die je samen met de internetdienstverleners uitwerkt. Er zijn verschillende typen versleuteling. De oplossing moet voor iedereen werkbaar en aanvaardbaar zijn. Dit is het verhaal. Dat is een delicate balans. Daar moet je zeer zorgvuldig mee omgaan. Dat doen wij ook.

De heer **Verhoeven** (D66):
Dank aan de Minister voor het neerzetten van zijn visie en zijn ervaring in Europa met dit onderwerp. Dit is natuurlijk zo'n onderwerp waarbij de technische situatie het wel zwart-wit maakt; de heer Van Dam zei het al. Daarmee bedoel ik dat je niet een beetje sterke encryptie kan hebben, zoals je ook niet een beetje anoniem kan zijn. «Anoniem» wil zeggen dat je echt totaal niet herleidbaar bent. Tegenwoordig wordt «anoniem» vaak gebruikt om mensen gerust te stellen, maar vervolgens is het door al die dataconnecties natuurlijk toch niet meer helemaal anoniem. Dat geldt ook hiervoor, denk ik. Je kunt zeggen: we willen sterke versleuteling, maar we willen toch ook wel iets in het opsporingsbelang kunnen doen. Dan hoor je vaak het woord «balans», «adequaat» of zo. Ik weet absoluut – de Minister kent mij goed genoeg om te weten dat ik dat ook meen – dat de Minister op een oprechte manier aan het zoeken is om die twee zaken te verbinden. Alleen hebben we de afgelopen kabinetsperiode toch wel een keer of drie, vier meegemaakt dat ik dan via het circuit te horen kreeg dat er toch weer plannen waren om die encryptie op een bepaalde manier te verbreken. Mijn eerste vraag is: wat zijn nou de conclusies van al die gesprekken met betrekking tot de mogelijkheden om een gebalanceerde aanpak te vinden? Is die gebalanceerde aanpak er wel? Of doorbreek je daarmee de facto encryptie?

Minister **Grapperhaus**:
Daar kan ik op dit moment nog geen antwoord op geven, omdat we dat nog niet weten. Ik heb zelf dit steeds uitgedragen. Dit is ook echt hoe het kabinet daarin zit. Laten we heel duidelijk en eerlijk zijn. Ik heb dat ook als speerpunt opgepakt. Bij kinderpornografie en kindermisbruik online spelen allerlei dingen als vrijheid van meningsuiting wat mij betreft geen rol, nul. Als iemand zegt dat hij dat wel vindt, dan moet ik dat maar horen. Zo is mijn introductiegesprek ook geweest met de grote techbedrijven en met de EU, met de Commissie. U hoort mij steeds zeggen «de EU». We moeten echt kijken hoe we dit samen kunnen oplossen ten behoeve van iedereen, alle EU-burgers en -bedrijven. We zien daar echt een grote,

akelige misstand die als een soort brij, ook sinds ik Minister ben – dat geef ik onmiddellijk toe – nog steeds verder aan het uitdijen is. Ik wou zeggen «uitbreiden», maar dat is wat ingewikkeld voor een brij. Daar moeten we dingen op kunnen bedenken om te voorkomen dat de encryptie ons in de weg zou zitten om volstrekt gerechtvaardigd te voorkomen dat een heel groot maatschappelijk kwaad zich verder verspreidt of er überhaupt is. Maar dan kom je op het punt – daar vinden we elkaar onmiddellijk; dat heb ik net gezegd – dat encryptie echt van wezenlijk belang is, ook voor de bescherming van een aantal fundamentele rechten in de digitale wereld. Dat is iets heel ingewikkelds. Ik zeg eerlijk dat ik de technische oplossingen die beide belangen echt goed respecteren nog niet voorbij heb zien komen. Daar zullen we dus nog steeds met elkaar naar moeten kijken. Ik vrees wel dat ik van de positieve instellingen ben. Als ik zie hoe de technologie ons in de afgelopen eeuw op allerlei andere punten wel heel veel dingen heeft gebracht, dan zou het wat mij betreft echt mogelijk moeten zijn om uiteindelijk wel degelijk technische oplossingen te vinden die, zoals ik al zei, de encryptie voor de burgers en bedrijven van goede wil volledig beschermen.

De heer **Verhoeven** (D66):
Ik krijg heel veel telefoontjes, whatsappjes, mailtjes en reacties op Twitter van allerlei technische mensen die elke keer tegen mij zeggen: Kees, er is op dit moment gewoon nog geen technische oplossing om op een veilige manier encryptie te doorbreken, dus trap er niet in; het is een bezweringsformule, het is cosmetica, het is typische veiligheidsretoriek, om het maar even wat negatiever te zeggen. Dus als er echt gezocht wordt naar technische oplossingen en de conclusie is «we hebben de technische oplossingen nog niet gevonden», dan denk ik dat dat voor nu een goede conclusie is. Ik denk dan in ieder geval: die oplossing is er nu niet, ik zie die niet en de Minister ziet die in de toekomst misschien wel omdat hij optimistisch is. Dat is denk ik ook een hele goede instelling.
Dan mijn tweede vraag. Er wordt heel vaak gezegd: we moeten die encryptie op de een of andere manier verbreken, want we verzamelen al die data; dat mogen we als diensten en als politie, maar vervolgens kunnen we ze niet lezen. Daardoor is er nu een verschuiving van het verzamelen van data naar het gebruiken van kwetsbaarheden om op die manier in computers te komen. Dat doen we dan via die zerodays. Daarvan heeft mijn fractie dan ook gezegd: daar moet je niet principieel nee tegen zeggen; dat gebruik moet mogelijk zijn, maar op een weloverwogen manier. Kijkt de Minister in het wat bredere discours over de verschillende middelen van opsporings- en inlichtingen- en veiligheidsdiensten om data af te tappen ook naar andere manieren om aan die informatie te komen, die er natuurlijk wel zijn? Zoekt hij ook naar mogelijkheden buiten de technische oplossing van encryptie? Daar ligt misschien ook een oplossingsrichting.

Minister **Grapperhaus**:
Bij alles in het digitale domein houd ik als kompas aan dat wat offline geldt ook online het uitgangspunt, de regel moet zijn. Dat betekent dat de afwegingen in het kader van rechtsstatelijkheid zowel offline als online moeten plaatsvinden. Dat geldt voor al die problematieken... Als ik erdoorheen praat, moet u het zeggen. O, dat mag weer niet. Maar goed, ik hoop het antwoord helder is. Ik begrijp dat wij binnenkort nog verder komen te spreken over zerodays. Maar ik vind dat als we offline rechtsstatelijke principes hebben, we die uiteraard ook online hebben. Overigens kun je best nog eens met elkaar een debat hebben over hoe die principes dan uitwerken, maar dat maakt democratie zo mooi.

De **voorzitter**:

Hartelijk dank. Excuses voor de kleine storing, maar ik was bezig om te voorkomen dat we nog een tweede termijn nodig hebben. Ik was dus ook in uw belang aan het werk. Als mevrouw Buitenweg nog een vraag mag stellen – ik kijk ook even naar de heer Verhoeven – dan heeft zij geen behoefte aan een tweede termijn. Die gun ik haar graag. O, de heer Verhoeven heeft ook nog een vraag. Laten we dat dan doen. Dan mogen we het ook een tweede termijn noemen; dat maakt allemaal niet zo veel uit. Mevrouw Buitenweg, gaat uw gang voor uw tweede termijn.

Mevrouw **Buitenweg** (GroenLinks):
Dank u wel, meneer de voorzitter. De heer Verhoeven en ik begonnen heel kort een discussie over de kern van het internet en de protocollen. Dat is hier verder ook niet voorbereid. We hebben er ook geen stukken over, maar ik zie daar eigenlijk nooit stukken over, terwijl ik denk dat die protocollen ook impact hebben op de veiligheid van het internet. Ik vraag me af op welke wijze wij als parlement geïnformeerd kunnen worden over wat de inzet van Nederland is ten aanzien van al die verschillende organisaties, zoals de IETF, en bijvoorbeeld ten aanzien van het voorstel van China voor het nieuwe IP. Op welke wijze gaan we die discussie ooit voeren in een parlement?

De **voorzitter**:
Dank u wel. Mevrouw Yeşilgöz.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Voorzitter. Ik wil alleen een VAO aanvragen. Dat is alles.

De **voorzitter**:
O, oké. Meneer Van Dam nog? Nee. Meneer Verhoeven.

De heer **Verhoeven** (D66):
Ik wil de Minister bedanken voor zijn antwoorden. Ik hoop dat hij nog één vraag van mij wil beantwoorden, namelijk de vraag of ik de komende maanden dan mag verwachten dat er nu een soort relatieve rust ontstaat op het encryptiedossier, in die zin dat de zoektocht naar technische oplossingen voorlopig weer even in een koelkast is gebracht en dat we over twee weken dus niet weer de ene of andere brief, discussiestuk of «onderhuidspaper» krijgen waaruit blijkt dat er toch weer nagedacht wordt over bepaalde vormen. Dat is me in deze kabinetsperiode een paar keer gebeurd en dat verontrust me. Daarom is de discussie misschien scherper dan zoals we die hier nu net hebben uitgewisseld. De heer Van Dam kijkt daar bedenkelijk bij, maar ik denk dat ik hier gewoon een goed punt maak.

De heer **Van Dam** (CDA):
Dat klinkt voor mij een beetje als: we moeten stoppen met denken. Laat ik op z'n minst zeggen dat ik iets meer verduidelijking van de heer Verhoeven wil hebben over wat hij daarmee precies bedoelt. Laat ik het als volgt zeggen. Je hebt encryptie en daar kun je aan gaan sleutelen. Je hebt zerodays. Maar ik heb me er echt in verdiept en er zijn natuurlijk ook allerlei andere manieren waarop je kunt zorgen dat je als overheid gewoon in de telefoon van de boef terechtkomt. Dat leest u trouwens ook in de boeken die u hier aanhaalt. Een ultiem voorbeeld is EncroChat en wat daar gebeurt. Ik zou het dus een buitengemeen treurige aangelegenheid vinden als ook dat soort ontwikkelingen on hold worden gezet, want dan zeggen we tegen de criminaliteitsbestrijders dus eigenlijk: de boeven mogen wel door, maar jullie even niet. Dat wil ik wel duidelijk hebben.

De heer **Verhoeven** (D66):

Stoppen met denken zou ik nooit iemand willen aanraden. Daar hoeft de heer Van Dam dus niet bang voor te zijn. Nee, mijn punt is het volgende. Ik heb net geschetst dat je als inlichtingen- of veiligheidsdienst op verschillende manieren aan informatie kan komen. Dat kan je doen met het verzamelen van data; daar ging het de afgelopen jaren de hele tijd over. Daarbij lopen we volgens sommige mensen een beetje vast op encryptie, maar bij de diensten en de politie is het allang verschoven naar hacken. Hacken kan je op verschillende manieren doen. Dat kan je doen door social engineering. Je kan mensen dus verleiden en zo bij ze binnenkomen. Dan heb je niet eens softwarefouten nodig. Maar je kan ook al dan niet onbekende softwarefouten gebruiken, zerodays, en dan kun je ook weer heel veel informatie achterhalen. Daar wordt op dit moment veel gebruik van gemaakt. Laten we nu dus niet doen alsof daar niet allerlei nieuwe gedachten, steeds verdergaande bevoegdheden en operationele aanpakken van diensten zijn ontstaan, want dat is wel degelijk gebeurd, terwijl er tegelijkertijd blijkbaar dus ook nog continu heel erg wordt nagedacht over technische oplossingen voor encryptie. Dat nadenken mag wel, maar als je bij elkaar komt als regeringsleiders of ministers en vervolgens toch wel heel vergaande dingen gaat opschrijven in notities, dan vind ik dat wel iets meer dan nadenken. Ik zou willen zeggen: zullen we nu even een soort politieke rust inbouwen om te voorkomen dat we elkaar elke keer opnieuw de hele tijd aan het opjutten zijn, terwijl het steeds op hetzelfde neerkomt, namelijk «we hebben de technische oplossing nog niet gevonden»? Dat is eigenlijk mijn punt.

De **voorzitter**:
Meneer Van Dam; het hoeft niet.

De heer **Van Dam** (CDA):
Dan vat ik het zo op dat de opmerking van de heer Verhoeven vooral ziet op het encryptiegedeelte sec en niet op andere dingen.

De heer **Verhoeven** (D66):
Ik kan daar met een lang exposé op reageren, maar het antwoord is eigenlijk gewoon ja.

De **voorzitter**:
Kijk, helder. Het woord is aan de Minister van Justitie en Veiligheid voor zijn tweede termijn.

Minister **Grapperhaus**:
Voorzitter. In het EZK-domein zit de discussie over de internationale internetgovernance. Gezien het feit dat het NCSC hier is ondergebracht, zou het op zich misschien te overwegen zijn om in een volgende kabinetsperiode daar een meer gedeelde verantwoordelijkheid van te maken, maar dat is nu dus niet zo. Nu ligt het in ieder geval op deze manier.

Mevrouw **Buitenweg** (GroenLinks):
Het punt is dat voor EZK een betere dienstverlening heel erg speelt. In het protocol kunnen daar een aantal keuzes voor worden gemaakt, maar dat kan soms strijdig zijn met zaken die dienstbaar zijn aan de cyberveiligheid. Dus ik wil aan deze coördinerende Minister vragen om enig zicht te houden op hoe de Staatssecretaris daar invulling aan geeft. Bij wat ik heb gezien is dat alleen heel zuiver gericht op dienstverlening. Ik zou dus op een gegeven moment willen weten op welke wijze Nederland invulling gaat geven aan die protocollen ten aanzien van cyberveiligheid en mensenrechten.

Minister **Grapperhaus**:

Ik begrijp dat heel goed, maar wij waren drieënhalf jaar geleden nog niet zover in ons denken dat we ons realiseerden dat internetprotocollen en internetgovernance inmiddels in heel grote mate gaan over cyberveiligheid en alles wat eromheen zit. Ik kan me voorstellen dat uit de formatie komt dat dat veel meer een invulling vanuit Justitie en Veiligheid zou moeten krijgen.
Voorzitter. Het punt van de heer Verhoeven heb ik gehoord. Encryptie staat volgende week ook op de agenda van de JBZ-Raad, de EU-Raad van de ministers van Justitie en Binnenlandse Zaken. Dan wordt er gesproken over de technische mogelijkheden en hoe wij daar goed onderzoek naar kunnen doen. Juist omdat ik net het belang van encryptie heb onderstreept, moeten wij niet stil blijven zitten maar ervoor zorgen dat wij in die discussie goed verdergaan. Ik denk dat wij zo echt met elkaar verder komen. Dat is een van de overwegingen geweest, die de heer Verhoeven ook kent, waarom het kabinet een jaar geleden heeft besloten om niet mee te gaan in de brief van Minister Barr en de Five Eyes: Nieuw-Zeeland, Canada, Australië, het Verenigd Koninkrijk en de Verenigde Staten. Maar goed, ik ga te veel daarnaartoe terug. Ik denk dat wij niet moeten stilzitten, maar de uitgangspunten heb ik net zeer nadrukkelijk uitgesproken, for everyone to hear and see.

De heer **Verhoeven** (D66):
Dat klopt. De Minister gaat naar die JBZ-Raad. Daarvoor controleert de Kamer altijd zijn inzet. Ik heb de agenda niet paraat, maar is daar nog een debat over of heeft dat al plaatsgevonden? Is het fiche, de inzet van Nederland, al bekend?

Minister **Grapperhaus**:
Daar is een schriftelijk overleg over.

De heer **Verhoeven** (D66):
Ah, schriftelijk.

Minister **Grapperhaus**:
Dat is al geweest volgens mij, ja. Maar ik wil de heer Verhoeven geruststellen, want wij staan altijd met open vizier tegenover elkaar. Die inzet is conform de uitgangspunten die ik net geschetst heb. We kijken echt met heel behoedzame tred wat er mogelijk is. We doen geen zaken die afbreuk doen aan de uitgangspunten die ik net schetste.

De **voorzitter**:
Dank u. Ik neem nog even de toezeggingen met u door. Dat is een hele lijst.
- De Minister van Justitie en Veiligheid informeert de Kamer jaarlijks over de testprogramma's in de voortgangsrapportages.
- De Minister van Justitie en Veiligheid informeert de Kamer begin volgend jaar over de wettelijke mogelijkheden om beter in kaart te krijgen welke systemen er worden gebruikt in de private sector.
- De Minister van Justitie en Veiligheid informeert de Kamer in de brief «pas toe of leg uit» ook over de centrale inkoop van cybersystemen door de departementen.
- De Minister informeert de Kamer begin volgend jaar over de statelijke actoren.
- De Minister informeert de Kamer over het voorstel van een cyberweerbericht. Is dat voor het verkiezingsreces? Even kijken. Nee. Dat gaat over de laatste toezegging, denk ik.
- De Minister informeert de Kamer voor het verkiezingsreces over de voortgang van het landelijk dekkend stelsel.

– De Minister informeert de Kamer begin volgend jaar over de vraag of HashCheckServices eenvoudig te manipuleren zijn en over de stand van zaken in Europees verband bij de aanpak van kinderporno.
– Ten slotte, de Minister van Justitie en Veiligheid informeert de Kamer over het overdragen van de systemen van grenscontroles aan de Schiphol Group in de brief met de reactie op het rapport van de Algemene Rekenkamer over cyberveiligheid bij het grenstoezicht op Schiphol.

Ten slotte is er een VAO aangevraagd met als eerste spreker mevrouw Yeşilgöz. Mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Ik denk dat een van uw conclusies niet helemaal juist geformuleerd was. Ik zag ook bij de ambtelijke staf wat verwarring. Volgens mij ging het erom dat wij bij private bedrijven willen bekijken wat de situatie is ten aanzien van losgeld en hoe vaak er losgeld wordt betaald. Het andere was om bij het NCSC te kijken naar «pas toe of leg uit».

De **voorzitter**:
Ik zie instemming. Ja? Dat klopt. Dan gaan we dat zo toevoegen. Zeer bedankt. De heer Van Dam nog.

De heer **Van Dam** (CDA):
Mag ik nog één vraag stellen aan mevrouw Yeşilgöz? Zij vraagt nu een VAO aan. De Minister heeft een brief toegezegd, ik meen in januari. Zou het een idee zijn om dat VAO te plannen na die brief? Dat biedt andere Kamerleden ook de mogelijkheid om dat VAO te benutten als dingen bij wijze van spreken niet uit de verf komen.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Ik vind het prima als het VAO na het kerstreces wordt gepland. Als de Minister vlak na het kerstreces met zijn brief komt, dan is het prima. Ik wil niet met het VAO wachten totdat die brief er een keer is. Hij is in januari toegezegd. Ik ga ervan uit dat dat half januari kan zijn, zodat we...

Minister **Grapperhaus**:
Nou, ik heb gezegd voor... Excuus, want ik onderbreek nu een lid, maar ik heb gezegd voor het februarireces. Ik weet niet of het mij eerder lukt. Dat weet ik gewoon echt niet. Laten we afspreken dat ik alles op alles ga zetten om eind januari met die brief te komen. Dan kunt u begin februari een VAO doen.

Mevrouw **Yeşilgöz-Zegerius** (VVD):
Laten we, als u het niet erg vindt, dat VAO dan wel in januari plannen.

Minister **Grapperhaus**:
Nou ja, wat u wil.

De **voorzitter**:
Ja, oké. Dat gaan we doorgeven aan de plenaire griffie. Het is niet anders, meneer Van Dam.
Goed. Daarmee komen we aan het eind van dit algemeen overleg. Ik dank de Minister, zijn ambtenaren, de leden, onze onvolprezen ondersteuning in alle mogelijke gedaanten en degenen die dit debat hebben gevolgd. Ik wens u allen nog een mooie dag. Ik sluit de bijeenkomst.

Sluiting 16.54 uur.