Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 807

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 20 december 2021

De vaste commissie voor Digitale Zaken heeft op 1 december 2021 overleg gevoerd met de heer Blok, Minister van Economische Zaken en Klimaat, de heer Grapperhaus, Minister van Justitie en Veiligheid, en de heer Knops, Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, over:

- **de brief van de Minister van Justitie en Veiligheid d.d. 11 juni 2021 inzake WODC-rapport «Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda (NCSA)» (Kamerstuk 26 643, nr. 763);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 11 juni 2021 inzake resultaat van voorafgaande raadpleging inzake Google (Kamerstuk 26 643, nr. 762);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 5 februari 2021 inzake recente ontwikkelingen rondom de hack op het Amerikaanse bedrijf SolarWinds (Kamerstuk 26 643, nr. 740);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 17 december 2020 inzake governance van het cybersecuritystelsel en de bescherming van vitale infrastructuur (Kamerstuk 26 643, nr. 732);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 29 juni 2021 inzake samenhangend inspectiebeeld cybersecurity (Kamerstuk 26 643, nr. 769);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 28 juni 2021 inzake beleidsreactie Cybersecuritybeeld Nederland 2021 (CSBN2021) en voortgangsrapportage van de Nederlandse Cybersecurity Agenda (NCSA) (Kamerstuk 26 643, nr. 767);**
- **de brief van de Staatssecretaris van Economische Zaken en Klimaat d.d. 16 december 2020 inzake voortgang van het Digital Trust Center (DTC) (Kamerstuk 26 643, nr. 742);**
- **de brief van de Staatssecretaris van Economische Zaken en Klimaat d.d. 14 december 2020 inzake voortgang Roadmap Digitaal Veilige Hard- en Software (Kamerstuk 26 643, nr. 735);**
- **de brief van de Minister van Economische Zaken en Klimaat d.d. 19 mei 2021 inzake wijziging naam vitaal proces (Kamerstuk 26 643, nr. 759);**

kst-26643-807
ISSN 0921 - 7371
's-Gravenhage 2021

- **de brief van de Staatssecretaris van Economische Zaken en Klimaat d.d. 2 juni 2021 inzake voortgang Digital Trust Center (Kamerstuk 26 643, nr. 760);**
- **de brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties d.d. 5 februari 2021 inzake voortgang diverse toezeggingen ICT en informatiebeveiliging binnen de Rijksdienst (Kamerstuk 26 643, nr. 739);**
- **de brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties d.d. 18 maart 2021 inzake voortgang informatieveiligheid bij de overheid (Kamerstuk 26 643, nr. 749);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 3 februari 2021 inzake uitkomsten verkenning wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten (Kamerstuk 26 643, nr. 738);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 14 september 2021 inzake evaluatie cyberoefening ISIDOOR 2021 (Kamerstuk 26 643, nr. 781);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 16 juli 2021 inzake voortgang toezegging en opvolging van de ARK-aanbevelingen inzake cybersecurity grenstoezicht Schiphol (Kamerstuk 26 643, nr. 774);**
- **de brief van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties d.d. 8 oktober 2021 inzake reactie op de motie van het lid Yeşilgöz-Zegerius over het opstellen van een cyberverdedigingsprotocol (Kamerstuk 26 643, nr. 786).**

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

De fungerend voorzitter van de commissie,
Leijten

De griffier van de commissie,
Boeve

Voorzitter: Leijten
Griffier: Boeve

Aanwezig zijn zeven leden der Kamer, te weten: Amhaouch, Dassen, Van Ginneken, Kathmann, Leijten, Rajkowski en Van Weerdenburg,

en de heer Blok, Minister van Economische Zaken en Klimaat, de heer Grapperhaus, Minister van Justitie en Veiligheid, en de heer Knops, Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

Aanvang 14.01 uur.

De **voorzitter**:
Ik open de vergadering van de vaste commissie voor Digitale Zaken voor het commissiedebat over online veiligheid en cybersecurity. Ik heet iedereen van harte welkom bij dit allereerste officiële debat van de commissie Digitale Zaken, met drie bewindspersonen. Demissionaire bewindspersonen, hoor ik dan te zeggen. Ik heet van harte welkom de Minister van Justitie, de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en natuurlijk hun ondersteuning. En ik heet van harte welkom de leden van deze Kamer, mevrouw Rajkowski van de VVD, mevrouw Van Weerdenburg van de PVV, mevrouw Van Ginneken van D66 en de heer Amhaouch van het CDA. Ik zal zelf het woord voeren namens de SP-fractie. Mogelijk komen er nog meer leden binnen. Die zal ik dan tussentijds welkom heten als er een gepast moment is. Dan geef ik mevrouw Rajkowski het woord voor haar woordvoering in eerste termijn.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Wat goed dat we het over dit onderwerp hebben en dat we met zo veel mensen bij elkaar zitten, want de digitale dreiging is een van de grootste veiligheidsvraagstukken van deze tijd. Daar hebben we het in de Tweede Kamer nog niet vaak genoeg over gehad. Daarom heb ik dit debat aangevraagd.
Voorzitter. Ik begin met ransomwareaanvallen. Je kunt de krant bijna niet openslaan of je ziet een aanval voorbijkomen, bijvoorbeeld bij het ROC Mondriaan, de HAN, Hof van Twente, VDL of MediaMarkt. En dan weten we ook nog dat niet alles in de media komt van bedrijven of instellingen die digitaal onder vuur liggen. Hoewel de schade vaker groter is als jouw bedrijf gegijzeld wordt door een digitale crimineel dan wanneer een dief er met de dagopbrengst vandoor gaat, zien we toch nog dat bedrijven zich wel goed fysiek weten te beveiligen, maar digitaal nog niet zo.
Voorzitter. De impact van een ransomwareaanval wordt niet meer onderschat door bedrijven, maar wel de kans dat het henzelf kan overkomen. Voorkomen is beter genezen. Ook daarbij is een rol weggelegd voor de overheid. De schade voor slachtoffers van ransomware is namelijk enorm en raakt de economie in het hart. Daarom is het zo belangrijk dat er meer informatie met ondernemers wordt gedeeld over aanstaande dreigingen. Sinds de zomer deelt het DTC al meer informatie. Het gaat om zo'n 300 bedrijven. Dat klinkt als heel veel. Het is ook een mooie eerste stap, maar in Nederland hebben we bijna 2 miljoen bedrijven, dus dan klinkt 300 al als wat minder. Dus graag daar wat vaart mee. Hoe gaat het kabinet ervoor zorgen dat meer bedrijven van deze goede informatie gebruik kunnen maken? Kan het kabinet aan de Autoriteit Persoonsgegevens vragen of ze haast wil maken met het wetsvoorstel dat gaat regelen dat IP-adressen gedeeld mogen worden tussen het NCSC en het DTC? Ik vind het in ieder geval lastig uitlegbaar dat bedrijven soms schade oplopen, terwijl deze informatie allang bekend is bij de overheid maar nog niet gedeeld mag worden.
Voorzitter. Dan heb ik vragen over een keurmerk. Want wat zou het helpen als duidelijk is met welke IT-dienstverlener je veilig zaken kunt doen. Er

speelt nu van alles rondom keurmerken. Je hebt de ISO-certificering, de cybersecurityverordening vanuit Europa en allerlei private initiatieven. Mijn vraag aan het kabinet: hoe voorkomen we een wildgroei aan keurmerken?
Voorzitter. Ik wil graag vragen of het kabinet kan ingaan op structureel oefenen met cyberdreigingen. Er is al vaker een oefening gedaan, maar nog niet grootschalig of vaak genoeg. Er heeft geloof ik vier jaar tussen de ISIDOOR-oefeningen gezeten. Dat mag nog wel wat structureler. Daar krijg ik graag een reactie op.
Dan als laatste onderwerp desinformatie. Vroeger haalden we in Nederland onze schouders op over desinformatie. Sinds de coronacrisis is duidelijk geworden wat stelselmatig verspreiden van desinformatie betekent voor het vertrouwen in onze instituties, politici en journalisten. We weten er alleen nog te weinig van af. Desinformatie aanpakken mag ook niet doorslaan naar censuur. Hoe doen we dat dan? Daarom heb ik de volgende vragen aan het kabinet. Kan het kabinet een openbaar onderzoek doen naar de omvang en de werking van desinformatie in Nederland? Wellicht zijn de aankomende gemeenteraadsverkiezingen daar een mooie aanleiding voor. Kan de Minister zich in Europa er hard voor maken om rapportages te krijgen over desinformatie die op socialmedia-platformen wordt verspreid? Ik weet dat er nu een praktijkcode is tussen de Europese Commissie en een aantal socialmediaplatformen. Ik zou graag zien dat een deel van die informatie ook met Nederland gedeeld wordt, zodat wij kunnen nadenken over welke tegencampagne wij eventueel kunnen voeren. Graag een toezegging.
Voorzitter. Dan de laatste vraag: is onze wet- en regelgeving eigenlijk wel klaar voor desinformatie maar ook voor deepfakevideo's? Als iemand slachtoffer wordt van een deepfakevideo, waar kan iemand dan een melding doen? Waar kan iemand aangifte doen? Kan dat bij de politie? Dat zijn allemaal vragen. Is ons stelsel er klaar voor? Dank u wel.

De **voorzitter**:
Dank u wel. Dan heet ik ook mevrouw Kathmann van de Partij van de Arbeid en de heer Dassen van Volt van harte welkom. Dan heeft mevrouw Van Ginneken een vraag voor mevrouw Rajkowski.

Mevrouw **Van Ginneken** (D66):
Dank aan collega Rajkowski. Mooi dat u zich uitspreekt tegen desinformatie. Ik zag u vanochtend bij Goedemorgen Nederland. Daar vertelde u al dat het belangrijk is dat de overheid tegencampagnes, voorlichtingscampagnes kan doen bij desinformatie. Ik vind dat een passend en goed idee, maar ik vraag me wel af of het genoeg is, gelet op hoe die platforms werken en hoe zij desinformatie en polarisatie versnellen. Kunnen we dan wel winnen met een voorlichtingscampagne?

Mevrouw **Rajkowski** (VVD):
Nee, zeker niet. Dat zit 'm ook in zorgen dat onze jongeren en kinderen meer les krijgen in mediawijsheid: hoe kun je desinformatie herkennen? De telefoon is een soort verlengde geworden van ons lichaam. Weten we wel welke informatie via dat scherm tot ons komt, van wie die is en met welk doel? Ik weet dat mevrouw Van Ginneken samen met de VVD en het CDA een hoorzitting heeft aangevraagd met de platformen. Ik ga graag met hen in gesprek over dat zij meer hun verantwoordelijkheid moeten pakken om te voorkomen dat desinformatie wordt verspreid. Het is een heel pakket aan maatregelen. Als mevrouw Van Ginneken daar nog meer ideeën voor heeft, sta ik daar graag voor open, want zo makkelijk komen we er niet.

Mevrouw **Van Ginneken** (D66):

Eén idee wil ik in ieder geval wel bespreken. We hebben in eerder verband ook gesproken over het tegengaan van illegale content. Hoe kijkt de VVD aan tegen maatregelen om ook schadelijke content te laten beperken op deze grote platforms?

Mevrouw **Rajkowski** (VVD):
Ik denk dat dat een van de onderwerpen is waarop VVD en D66 verschillen. Schadelijke content kan zoveel meer zijn. Dat kan ook een vervelende opmerking zijn, pesten, iemand die iets als een belediging ervaart wat misschien niet zo bedoeld is of wat door iemand anders niet als een belediging wordt ervaren. Voor de VVD is het zo belangrijk dat we bij het aanpakken van desinformatie voorkomen dat er censuur gaat ontstaan. Op het moment dat je die schadelijke content gaat aanpakken, wordt het echt veel te subjectief wat wel en niet schadelijk is. Daar zou ik graag verre van willen blijven.

Mevrouw **Van Ginneken** (D66):
Ik laat het hierbij.

De **voorzitter**:
Mevrouw Van Weerdenburg van de PVV, uw termijn.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Vandaag is het dan eindelijk zover: het allereerste officiële debat van de langverwachte vaste commissie voor Digitale Zaken. Er is ongelofelijk lang naartoe gewerkt door een heleboel mensen. Ik had het voorrecht om een stukje van de voorgeschiedenis te begeleiden als lid van de tijdelijke commissie Digitale toekomst, die aan de basis stond van deze vaste commissie voor Digitale Zaken. We zijn inmiddels ruim een halfjaar geleden ingesteld, maar dan nu eindelijk het eerste volwaardige debat.
Het is jammer dat we dit debat niet kunnen houden met de Minister voor Digitale Zaken in een missionair kabinet. Dat was in ieder geval de voorkeur geweest van de PVV. Maar de formerende partijen tonen geen enkele urgentie om tot een nieuw landsbestuur te komen. Dat is onbegrijpelijk, want het onderwerp van dit debat, online veiligheid en cybersecurity, vraagt om daadkracht en regie. De mensen die dit debat thuis volgen en de indrukwekkende hoeveelheid stukken zien die vandaag op de agenda staan, zouden zomaar eens de indruk kunnen krijgen dat die daadkracht en regie er in Nederland is en dat we het hier supergoed geregeld hebben.
Het gaat over lijvige rapporten, zoals bijvoorbeeld de Nederlandse Cybersecurity Agenda, het Cybersecuritybeeld Nederland 2021, het rapport Samenhangend inspectiebeeld cybersecurity en de Roadmap Digitaal Veilige Hard- en Software. En over allerlei indrukwekkend klinkende instanties, zoals het Digital Trust Center, het WODC en de Cyber Security Raad. Bovendien zitten hier maar liefst drie bewindspersonen aan tafel, demissionaire bewindspersonen. Het lijkt alsof cyberveiligheid tópprioriteit is voor dit kabinet, totdat je bedenkt dat dit kabinet vooral met beeldvorming bezig is. Het is de illusie van daadkracht, een papieren werkelijkheid. Er wordt enorm veel vergaderd over cyberveiligheid en er wordt nóg meer over geschreven en gepubliceerd. Maar wat wordt er nou eigenlijk concreet gedáán?
Als de coronacrisis ons iets heeft laten zien, is het dat goed voorbereid zijn op papier iets heel anders is dan een daadwerkelijke crisis het hoofd kunnen bieden in de praktijk. In dat kader verwijs ik ook naar de leerpunten die zijn geformuleerd naar aanleiding van de cyberoefening ISIDOOR, die bevestigen dat de snelheid van de besluitvorming omhoog moet om de impact te kunnen beperken. Want als de nood aan de man is

en er snel en daadkrachtig gehandeld moet worden, heb je niks aan dikke rapporten en uitgebreide overlegstructuren.
Voorzitter. Ik kan u voorspellen dat de demissionaire Ministers die hier vandaag aan tafel zitten vaak gaan verwijzen naar de formatietafel. Ze zullen op onze zorgen en vragen antwoorden: dat is aan een nieuw kabinet. Dat hebben ze namelijk al vaker gedaan de laatste tijd. Ik verwijs maar even naar de begrotingsbehandeling van Justitie en Veiligheid van afgelopen week, waar de Minister van Justitie onder meer zei: «Of er een aparte Minister dient te komen voor cybersecurity met een ministerie-overkoepelende taak is aan een nieuw kabinet.» En: «Het volgende kabinet zal uiteindelijk moeten besluiten over een nieuwe cybersecurity- en cybercrime-aanpak en de financiering daarvan.» «Het is aan een volgend kabinet om te bezien hoe wordt voortgebouwd op de ervaringen die onder het huidige kabinet zijn opgedaan met de Nederlandse Cybersecurity Agenda (NCSA) en de aanpak van cybercrime.» «De conclusies uit deze rapporten van de CSR en het WODC zullen moeten worden betrokken bij het opstellen van een nieuwe strategie.»
U ziet, voorzitter, vandaag is dus een beetje voor de bühne. Dat had de PVV liever anders gezien. Als het aan ons ligt, gaan we vaart maken met de formatie en maken we cyberveiligheid direct chefsache. Stel een Minister aan voor Digitale Zaken met doorzettingsmacht en budget en laat die persoon direct aan de slag gaan met één heldere, eenduidige nationale cyberveiligheidsstrategie. Want de digitale dreigingen zijn reëel en urgent. Laten we niet wachten tot een cyberaanval de samenleving platlegt.
Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Van Weerdenburg. Dan geef ik het woord aan mevrouw Van Ginneken namens D66.

Mevrouw **Van Ginneken** (D66):
Dank u wel, voorzitter. Laat u niet misleiden door de bijvoeglijke naamwoorden. Cybersecurity en online veiligheid gaan over security of veiligheid, want wat er gebeurt in onze digitale ruimte heeft maar al te vaak gevolgen voor de fysieke ruimte, gevolgen voor de overheid en bedrijven, gevolgen voor u en mij. En vaak komen alleen de direct zichtbare gevolgen in het nieuws. Een school gesloten, geen kaas in de supermarkt, een digitale gijzeling met ransomware. Maar daaronder gaat iets fundamenteels schuil: onze kenniseconomie wordt bedreigd als onze bedrijven en kennisinstellingen kwetsbaar zijn voor digitale spionage. Onze maatschappij kan ontwricht worden door digitale sabotage, door statelijke actoren en criminelen. Cybersecurity heeft daarom wat D66 betreft topprioriteit.
Voorzitter. Om ons tegen digitale dreigingen te verweren, hebben we elkaar nodig. Overheid, bedrijven, kennisinstellingen, brancheorganisaties, het is een gezamenlijke verantwoordelijkheid waarbij we elkaar moeten informeren, steunen en helpen. Daar zal ik mij vandaag dan ook vooral op focussen. Onze overheid néémt een zichtbare rol, met het Nationaal Cyber Security Center en het Digital Trust Center, voor de mensen thuis: het NCSC en het DTC. Beide organisaties schitterden het afgelopen jaar. Het DTC – collega Rajkowski noemde het al – waarschuwde honderden bedrijven voor ernstige cyberdreigingen en het NCSC speelde een grote rol in het oppakken van ransomwarecriminelen in acht verschillende landen. Mijn complimenten daarvoor. Maar deze twee organisaties werken gescheiden, met verschillende opdrachten en onder verschillende Ministers: NCSC voor het Rijk en vitale sectoren en DTC voor de rest van de samenleving. Maar criminelen en statelijke actoren houden zich niet aan deze scheiding.

Dit weekend schreef de New York Times dat in Israël steeds vaker juist niet-vitale doelwitten gekozen worden, vaak minder goed beveiligd en dus makkelijk aan te vallen. Dit ontwricht ook de samenleving en zorgt voor gevoelens van onveiligheid bij de burger. Vele klappen maken immers ook een dreun.
Maar intussen hebben wij in ons land twee wettelijk gescheiden verdedigingslinies, de Wbni en de Wbdwb, de tongbreker. Deze beide wetten worden nu aangepast en de inbreng van bedrijven en specialisten hierop is vrij eensluidend: verzacht nu deze scheiding of laat hem helemaal vallen. Dat is een pleidooi dat ik van harte ondersteun. Daarom vraag ik de Minister: moet het NCSC niet minimaal de bevoegdheid krijgen om buiten de OKTT's om rechtstreeks organisaties te informeren ingeval van hoge urgentie of risico? Moet het onderscheid vitaal-niet vitaal dat nog steeds centraal staat in de cybersecurity-aanpak van het kabinet niet komen te vervallen? En moeten we niet toegroeien naar één organisatie met een integrale verantwoordelijkheid voor cybersecurity, zoals het NCSC in het Verenigd Koninkrijk?
Voorzitter. D66 hoort van mkb-bedrijven dat zij de kennis en capaciteit missen om goed weerbaar te zijn. Het DTC geeft goede maar algemene adviezen, terwijl sectorkennis juist zo helpt. D66 ziet dan ook een belangrijke rol weggelegd voor brancheorganisaties om hun leden specifieker te informeren en weerbaarder te maken. En toch is er maar een beperkt aantal sectoren met een Computer Emergency Response Team. Is de Minister bereid om brancheorganisaties op te roepen en te stimuleren sectorale CERT's op te richten?
Voorzitter. Ook als het gaat om het reageren op cyberaanvallen geldt: oefening baart kunst. De ISODOOR-oefeningen van de rijksoverheid en vitale sectoren zijn daarom nuttig. Ik las in de begroting voor volgend jaar dat de Minister deze jaarlijks wil gaan doen. Dat is een goed plan, wat D66 betreft. Maar ook hier is de vraag weer of deze oefeningen niet te beperkt worden ingezet. Ziet de Minister de mogelijkheid om ook meer bedrijven te betrekken bij deze oefeningen, bijvoorbeeld jaarlijks in een aantal roulerende sectoren? Ook vraag ik me af of de overheid wel snel genoeg leert van hacks. De Onderzoeksraad voor Veiligheid onderzoekt het Citrix-lek uit 2019 nu al twee jaar. Wanneer verwacht de Minister de resultaten van dat onderzoek en welke mogelijkheden ziet de Minister om dergelijke evaluaties sneller uit te voeren?
Dan nu over naar Pegasus-spyware. Deze zomer brak een groot schandaal uit rond deze spyware van het bedrijf NSO. Journalisten en mensenrechtenactivisten wereldwijd werden gehackt en gevolgd. Ook meerdere Europeanen waren slachtoffer. We weten inmiddels dat Frankrijk en Duitsland ook bijna NSO-software hebben aangeschaft. Mijn vragen zijn: hoe helpt onze overheid activisten, advocaten en journalisten zich te verweren tegen dit soort ondermijnende praktijken? Deelt het NCSC of de NCTV ook informatie met individuen als zij doelwit zijn? En heeft de Nederlandse regering ooit contact gehad met NSO of een aankoop overwogen? Zulke spywaresoftware maakt gebruik van zerodaykwetsbaarheden, onbekende kwetsbaarheden waar geen beveiliging tegen komt als die kwetsbaarheid onbekend blijft. Zulke zerodays worden ook gebruikt door onze politie. Door deze te kopen, houdt de politie een gevaarlijke industrie in stand. Hoe kijkt de Minister naar een verbod voor de politie om zerodays aan te schaffen?
Tot slot nog even over online veiligheid. Begin dit jaar verscheen een alarmerend stuk in De Groene Amsterdammer waaruit bleek dat vrouwelijke politici disproportioneel vaak te maken krijgen met online haat en bedreiging. Niet alleen politici, maar alle vrouwen krijgen te maken met online haat, zoals online geweld, online stalking, deepfakes en afpersing. Welke mogelijkheden ziet de Minister om online geweld tegen vrouwen aan te pakken? D66 zou graag zien dat we digitale bescherming voor vrouwen ook vastleggen in de Istanbul Conventie en dat ook naleven. Hoe

kijkt de Minister hier tegenaan? Ik kijk uit naar de beantwoording door de Minister.
Dank u wel.

De **voorzitter**:
Ik dank u wel. Dan geef ik het woord aan de heer Amhaouch namens het CDA.

De heer **Amhaouch** (CDA):
Voorzitter, dank u wel. Dit is inderdaad ons eerste commissiedebat en zo te horen is het misschien wel de commissie van afkortingen.

De **voorzitter**:
Het is goed dat u het zegt. Ik heb ze opgeschreven. Ik wilde ze aan het einde van het debat allemaal even verklaren.

De heer **Amhaouch** (CDA):
We gaan ze niet overhoren. Ik denk dat niemand vandaag zakt.

De **voorzitter**:
Wellicht betrap ik u er nog op. Ik zal u er niet op wijzen, maar dan neem ik ze mee in het afkortingenlijstje.

De heer **Amhaouch** (CDA):
Ik heb geprobeerd om ze te ontwijken.
Voorzitter. Goed dat we ons hier als commissie voor Digitale Zaken buigen over een van de grootste bedreigingen van onze veiligheid en toekomstige veiligheid, namelijk de digitale dreiging. Een dergelijk groot onderwerp vraagt meer spreektijd. Die hebben we vandaag gelukkig ook gekregen. Toch wil ik me beperken tot een aantal thema's. Ik wil het hebben over de dreiging van ransomware en over de vraag hoe daarmee om te gaan, de online veiligheid van burgers, de veiligheid van de overheid op digitaal vlak en ten slotte de cyberoefeningen.
Allereerst de problemen van ransomware. Dit punt is ook genoemd door collega Rajkowski. We hebben inderdaad de voorbeelden gezien van VDL en MediaMarkt. Maar nog veel erger, of in ieder geval heel kritisch, zijn de ransomaanvallen op ziekenhuizen in Nederland, België, Canada en Ierland. En dat terwijl we middenin een gezondheidscrisis zitten. Dat baart ons dus grote zorgen. Het is een almaar groter wordend probleem. Enerzijds hebben criminelen ontdekt hoeveel geld er relatief gemakkelijk te verdienen is. Anderzijds hebben statelijke actoren door hoe ontwrichtend de gerichte gijzeling van digitale systemen kan werken. In de Kamer is er hier en daar al veel over gediscussieerd. Dat is een relevante discussie, lijkt me. Maar kunnen de bewindspersonen van de verschillende departementen hier kort op reflecteren?
Voorzitter. Het is duidelijk dat bedrijven, overheid en burgers nog te weinig doen om hun digitale apparaten te beveiligen. Het is alsof we allen een eigen digitaal huis hebben gebouwd en pas sinds enkele jaren lijken te beseffen dat hang- en sluitwerk best wenselijk is. Criminelen grijpen in tussentijd hun kans. Dit geldt zowel in het groot voor de rijksoverheid en vitale sectoren, als in het klein voor de mkb-ondernemer of voor individuen die getroffen worden door de gijzelsoftware. Inmiddels heeft de meerderheid van de bedrijven in de afgelopen twee jaar te maken gehad met aanvallen.
Het CDA ziet een belangrijke taak voor de overheid om de veiligheid en de preventieve werking te bevorderen. Dat brengt mij ook bij het nu al veelbesproken verbod op het betalen van losgeld bij een ransomware-aanval en het idee dat we niet moeten beginnen aan een verzekering voor cyberaanvallen. Ik begrijp waar de Minister vandaan komt. Ik heb ook het liefst dat we deze criminelen geen cent geven. Maar het is onrealistisch

om te denken dat we met een verbod op losgeldbetalingen de gijzelsoftware-industrie een halt gaan toeroepen. Waarom kijken we niet naar verplichte cyberverzekeringen die bedrijven er ook toe bewegen dat dat zij hun cyberveiligheid op orde hebben? Wanneer je jezelf verzekert tegen brand, moet je ook aan de minimumeisen voor brandveiligheid voldoen om eventuele vergoedingen uitgekeerd te krijgen. Op deze manier kunnen ook verzekeringen juist helpen bij het tegengaan van gijzelsoftware op de lange termijn. Is er bij de Minister sprake van voortschrijdend inzicht en wil hij hiernaar kijken? Of houdt hij vast aan een verbod?
Voorzitter. Dan kom ik op de versnippering van het beleid voor cyberveiligheid. Beveiliging is zo sterk als de zwakste schakel; dat geldt ook voor het beleid op het gebied van veiligheid. Ik begrijp dat we te maken hebben met een uitgebreid overheidsorgaan en dat het primair de taak van organisaties zelf is om de veiligheid op orde te hebben. De Algemene Rekenkamer stelt ook dat de informatiebeveiliging nog niet op orde is. Whatsappaccounts van zowel Eerste Kamerleden als Tweede Kamerleden en ambtenaren van ministeries zijn door criminelen overgenomen. Bij het Ministerie van Buitenlandse Zaken was sprake van een mogelijk datalek. Het veilig gebruiken van applicaties voor videovergaderingen was onvoldoende gegarandeerd. Mijn partij pleit daarom voor een integrale langetermijnagenda voor cybersecurity en wil daarvoor een nationale coördinator aanstellen, om meer eenheid te krijgen in het beleid. Hoe zien de bewindspersonen dat?
Voorzitter. Ten slotte kom ik bij de evaluatie van de cyberoefening ISIDOOR 2021. Het is heel goed dat mooie woorden op papier vertaald worden naar de praktijk. Dan is oefenen en het doen van stresstesten een goed instrument. En dan is het ook echt hopen dat er zaken misgaan. Ik lees dat er meer dan 90 organisaties hebben meegedaan aan deze oefening van het Nationaal Crisisplan Digitaal, waarbij ook de eigen crisisprocedures van de deelnemende organisaties zijn getest. De Minister zegt hierover dat het rapport concrete en nuttige aanbevelingen bevat waarmee een nieuw kabinet de maatregelen ten behoeve van de versterking van de digitale weerbaarheid en de voorbereiding op een digitale crisis verder kan vormgeven. Tevens vraagt hij aan de deelnemende organisaties van ISIDOOR om ook zelf aan de slag te gaan met de eigen leerpunten uit deze oefening. Hierbij heb ik twee vragen. Wat is de staat van de overheid en de staat van de betrokken organisaties bij de crisisbeheersing? Wat zijn op dat punt de conclusies? Kunnen we die duiden? Ten tweede. Hoe staat het met de actualisering van het Nationaal Crisisplan Digitaal en de doorontwikkeling van dit plan tot een landelijk crisisplan naar aanleiding van deze oefeningen?
Dat waren weinig afkortingen, voorzitter.

De **voorzitter**:
Nee, ik heb er geen één bij gezet op het lijstje. Ik heb u in de gaten gehouden, meneer Amhaouch. Dan mevrouw Kathmann namens de Partij van de Arbeid.

Mevrouw **Kathmann** (PvdA):
Dank u, voorzitter. Het is een mooie week en ook wel een noodzakelijke week om als commissie dit eerste debat te voeren, want mijn week begon in ieder geval met de volgende mail, die gericht is aan álle politieke partijen. Apple heeft recent aan een aantal gebruikers een legitieme waarschuwing verstrekt over mogelijk misbruik van iPhones door zogenaamde statelijke actoren. Het dringend verzoek is om aan de leden en medewerkers van je fractie te vragen contact op te nemen met de CISO indien zij van Apple ook zo'n waarschuwing hebben ontvangen, ook als het een privétoestel betreft. Hier gaat het dus gewoon om het hacken van telefoons van politici door statelijke actoren. Ik vind dat nogal wat. Als ik

daarbij ook nog optel dat de site van de PvdA tijdens de afgelopen verkiezingen gewoon heeft platgelegen, mogelijk door een aanval vanuit Turkije, dan kan je wel zeggen dat cybercrime alomtegenwoordig en staatsgevaarlijk is.
Het is ook wel een beetje jammer dat we soms vergeten hoe veel het ook kan opleveren. We hebben best wel een cybersecurityeconomie met potentie, die ons aan de ene kant veel beter kan beschermen en aan de andere kant ook echt wat kan opleveren. Daarom moet ik mijn eerdere collega's toch even bijvallen. Als dit demissionaire kabinet zegt «we vinden het een ongelofelijke topprioriteit, juist omdat deze dingen kunnen gebeuren» en er dan dit bedrag tegenover zet, dan doet het niet echt aan «put your money where your mouth is». Ik hoop dat we daar in de toekomst echt veel meer van kunnen verwachten.
Dan ga ik snel naar de punten, want het is echt een brij aan stukken. Ik zal ze even stuk voor stuk aflopen. Ik heb een vraag over het WODC-rapport over de Nederlandse Cybersecurity Agenda. Daar zaten een paar stevige aanbevelingen bij. Mijn vraag aan de Minister is: hoe worden deze aanbevelingen meegenomen, zeker als het gaat om het opstellen van de toekomstige agenda?
Dan de hack op SolarWinds. Wat leert dat ons en wat doet het met ons als Nederland? De Minister geeft aan dat ook rijksdiensten gebruik hebben gemaakt van de kwetsbare software. Welke rijksdiensten zijn dat, en op welke punten was die software kwetsbaar? Er wordt wel gezegd dat er geen sporen van misbruik zijn, maar dat is natuurlijk tot nu toe. Welke kwetsbare informatie heeft er op straat gelegen en welke risico's lopen we dat die informatie in de toekomst alsnog naar buiten wordt gebracht? Ik zou daar graag meer over horen.
Er lag ook nog een ander stevig rapport, over de governance van het cybersecuritystelsel. Dat is een rapport van RAND. Dat heeft ook weer stevige aanbevelingen. Ik zou van de Minister graag punt voor punt willen horen wat hij met deze aanbevelingen gaat doen.
Ik heb het over de stevige rapporten gehad, maar we kunnen natuurlijk nooit al die aanbevelingen vlot trekken zonder goed opgeleide mensen. Ook vanuit Europa wordt daarover echt aan de bel getrokken. We hebben meer afgestudeerden nodig. Maar dit zie ik eigenlijk in geen enkel onderzoek of punt van aandacht heel goed terugkomen. Ik zou dus heel graag van de Minister willen horen hoe dat spoor van onderwijs, opleiden en personeelstekort in de toekomst veel duidelijker wordt opgenomen in de Cybersecurity Agenda en dus ook hoe hierin samen wordt opgetrokken met collega's van OCW en IenW.
Dan het Rekenkamerrapport over de cybersecurity op Schiphol. Dat was best wel een bizar Rekenkamerrapport. Als het niet was geschreven, dan was in ieder geval niet vlot getrokken dat mensen die kwaad wilden passagiersgegevens gewoon zo konden manipuleren dat bijvoorbeeld mensen die internationaal gezocht werden ineens niet meer op de passagierslijst stonden, maar zich wel op Schiphol bevonden. Voor mij is het in de reactie van de Minister niet echt duidelijk wat er nou wel en niet is opgelost. Er wordt wel gezegd: we hebben een soort diepteonderzoek gedaan en we hebben de meest urgente problemen daar opgelost. Maar ik zou heel graag willen weten welke problemen dat zijn. De Rekenkamer zelf had er een heel mooi stippenkaartje bij gezet. Het zou voor mij al heel veel schelen, of in ieder geval veel duidelijker zijn, als we ook op die manier door de Minister worden geïnformeerd. Zij hadden een kaartje. De stippen moesten groen zijn, want dan deed Schiphol het goed op het gebied van cybersecurity, maar van alle negen stippen was er maar één groen. Dat ging dus over wie zei welke cybersecuritymaatregelen er genomen moesten worden, óf die genomen waren, of er goedkeuring voor was gegeven, of er beveiligingstesten waren uitgevoerd. Alles stond op rood. Ik zou graag willen weten wat de status van die stippen is en of we nu gewoon negen groene stippen hebben.

Dan Clearing House. Dat is veel in het nieuws geweest. Het is een initiatief van internetgerelateerde organisaties dat waarschuwt bij cyberkwetsbaarheden. Het is een gezamenlijk platform van het bedrijfsleven dat waarschuwt voor cyberaanvallen. Het is dus eigenlijk iets wat het veld zelf is gaan optuigen, omdat het landelijk systeem dat ons moet waarschuwen voor hacks, het LDS – daar hebben we weer zo'n afkorting – voor hen niet voldoende is en ook niet voldoende snel wordt opgetuigd. Ik zou dus graag willen weten hoe de Minister hiernaar kijkt. Wordt er samen met Clearing House opgetrokken? Zo niet, waarom niet? En zo wel, hoe dan? Dit heeft natuurlijk ook van alles te maken met de rol van het DTC. Kan de Minister reflecteren op het idee om de werkzaamheden van het NCSC en ook het DTC uit te breiden? Dan zou het NCSC niet alleen over vitaal en Rijk gaan, maar ook over bedrijven met sleutelinnovaties en misschien wel het grote bedrijfsleven met – ik noem maar wat – meer dan 500 werknemers. Het DTC zouden dan zodanig kunnen opereren – andere collega's zeiden het al – dat informatie uitgewisseld kan worden, echt als hét loket voor het mkb, misschien zelfs wel met een soort van 112-nummer – dat kan ook gewoon digitaal ingeregeld worden – waar je in het geval van een cybercrisis naartoe kan bellen als je zo'n mkb'er bent. Denk ook aan een pool van ethische hackers, waar ook veel meer op crises getraind kan worden. Het is ongelofelijk duur om dat te doen, maar het moet wel gebeuren. Ik hoop dat de Minister deze plannen kan steunen en dat hij in ieder geval kan vertellen wat hij daarvan vindt.
Tot slot. Dan moet ik er eventjes een kiezen. Encryptie. Verschillende partijen hebben er voor de verkiezingen natuurlijk toe opgeroepen om het gebruik van encryptie te stimuleren. Via het lid Rajkowski hebben we een hele mooie kaart gekregen die ons helpt in de politieke discussie. Maar wat als uit die politieke discussie nou komt: we kunnen er niet aan sleutelen, om het maar zo te zeggen; het is zoals het is en we kunnen het niet afschalen? Hebben we dan alternatieven waardoor opsporingsdiensten toch op een goede manier aan hun informatie kunnen komen? Ik hoor graag van de Minister of die alternatieven er zijn.

De **voorzitter**:
Dank u wel, mevrouw Kathmann. Dan geef ik het woord aan de heer Dassen van Volt.

De heer **Dassen** (Volt):
Dank, voorzitter. De collega's noemden al wat voorbeelden. Weer een cyberaanval, dit keer op de MediaMarkt, zoals het Brabants Dagblad kopte. Of: «ROC Mondriaan meldt grote hack, studenten kunnen niet bij bestanden», zoals Tweakers schreef. Twee recente voorbeelden die illustreren wat de NCTV concludeert in het Cybersecuritybeeld Nederland 2021. Nederland is in de afgelopen periode geraakt door een breed scala aan cyberincidenten. Hoewel we spreken van incidenten, is de problematiek natuurlijk structureel. Volt heeft de blik op de toekomst. We zien veel kansen op het gebied van digitalisering. Digitalisering brengt de landen van Europa dichter bij elkaar, maar maakt ons ook kwetsbaarder. De aanwezige bewindspersonen spannen zich allen in voor een veiligere digitale omgeving. Dat wordt natuurlijk gewaardeerd, maar ik sluit me ook aan bij de collega's die eerder aangaven dat het nog onvoldoende is en dat er zeker wel een tandje bij kan.
Voorzitter. Er staat een hoop op de agenda. Ik ga me vandaag richten op drie onderwerpen: het verbeteren van onze cybersecuritystrategie, het Digital Trust Center en Europese samenwerking.
Voorzitter. In het begrotingsdebat van vorige week grapte de Minister dat er waarschijnlijk een hoop Kamerleden in de zaal zouden zitten met als pincode voor hun telefoon vier nullen, dus 0000. Ik vond dit een mooi en eenvoudig voorbeeld om de verschillende facetten van cybersecurity te omschrijven. Maar het geeft ook een beetje het niveau aan van de

volwassenheid van onze cybersecurityaanpak, terwijl de criminele cybereconomie inmiddels echt erg volwassen aan het worden is.
Voorzitter. Om het de bewindspersonen vandaag iets makkelijker te maken, verwijs ik graag even terug naar het regeerakkoord uit 2017. Daarin sprak het demissionaire kabinet uit om een ambitieuze cybersecurityagenda op te stellen en daar jaarlijks 95 miljoen euro voor vrij te maken. Dat is niet helemaal gelukt, zoals we kunnen zien. Daarom stelt Volt het volgende voor. Neem de bestaande Nederlandse Cybersecurity Agenda als uitgangspunt voor een strategie die op basis van een integrale aanpak met een duidelijke visie concrete en meetbare doelen stelt. Neem daarbij het advies van de Cyber Security Raad over en maak daarvoor de benodigde middelen vrij. Neem als overheid verantwoordelijkheid voor de cyberweerbaarheid van heel Nederland, dus niet alleen van de vitale sectoren en het Rijk, maar ook van Nederlandse burgers en andere bedrijven.
Voorzitter. Ik heb de volgende vragen. Wordt er op basis van het adviesrapport van de Cyber Security Raad, het WODC-rapport ter evaluatie van de Nederlandse Cybersecurity Agenda en de eigen ervaringen gewerkt aan het verbeteren van de huidige Nederlandse Cybersecurity Agenda? Zo ja, op welke manier? Zo nee, worden er dan technische voorbereidingen getroffen voor een verbeterde cybersecuritystrategie voor een nieuw kabinet? Kan er een schatting worden gemaakt van de jaarlijkse maatschappelijke en economische kosten van cyberincidenten? Hebben de Ministers kennisgenomen van de plannen voor onlineveiligheid en cybersecurity uit het regeerakkoord van de nieuwe Duitse coalitie?
Voorzitter. We moeten dit samen doen. Het Digital Trust Center is opgezet om Nederlandse bedrijven en organisaties te kunnen waarschuwen voor securitydreigingen. Daar heb ik een paar vragen over. Zijn er al ervaringen die gedeeld kunnen worden? Hoe is de samenwerking tussen het NCSC en het DTC? Welke belemmeringen voor samenwerking zijn er op dit moment nog en hoe kunnen die weggenomen worden? Wordt er in Europees verband gesproken over soortgelijke projecten? Zijn daar best practices voor opgehaald? Is er bijvoorbeeld gesproken met het Verenigd Koninkrijk over het Cyber Security Information Sharing Partnership? Ziet de Minister mogelijkheden om bijvoorbeeld het realtime delen van informatie, zoals bij het CiSP, ook bij het DTC mogelijk te maken? Dat sluit een beetje aan bij wat mevrouw Kathmann net zei: bedrijven wisselen daar op een platform realtime informatie met elkaar uit, zodat ze meteen op de hoogte zijn van de cyberdreigingen die overal spelen.
Voorzitter. Daarmee kom ik bij het laatste deel aan: Europese samenwerking. De Minister van Buitenlandse Zaken onderstreepte onlangs nog dat voor sterke cyberweerbaarheid internationale samenwerking noodzakelijk is. Onlangs hebben we antwoord gekregen op onze vragen over het BNC-fiche over de Joint Cyber Unit. We hebben daar ook de vraag gesteld of de Minister ruimte ziet om samenwerking in de Joint Cyber Unit te verplichten voor zover die niet op vrijwillige basis tot stand komt. Daar hebben we helaas nog geen antwoord op gekregen. Vandaar de volgende vragen. Zouden we daar alsnog antwoord op kunnen krijgen? Werkt een Joint Cyber Unit niet veel beter als iedereen daarbij aangesloten is?
Voorzitter. Ik zou graag willen afsluiten met een uitdaging aan de Ministers om gezamenlijk het volgende uiteen te zetten. Wat is hun visie op hoe onlineveiligheid en cybersecurity eruit horen te zien? Wat achten zij daarvoor nodig? Hoe verschilt veiligheid in het digitale domein van veiligheid in het fysieke domein volgens de Ministers?
Dank u wel.

De **voorzitter**:
Dank u wel. Dat leidt tot een vraag bij mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Ik zou al die vragen over visie en wat de verschillen zijn, terug willen leggen bij de heer Dassen. Hoe kijkt Volt daar dan tegenaan? Maar mijn interruptie gaat over iets anders, namelijk IP-adressen. De Autoriteit Persoonsgegevens zou zomaar IP-adressen als een persoonsgegeven kunnen zien, en dat maakt juist het delen van dreigingen tussen NCC en DTC zo lastig. Nu zijn we nog aan het wachten op een wetsvoorstel. Eerst moet de AP daar nog wat van vinden, dan gaat het naar de Raad van State en daarna komt het pas naar ons. Is dit dan een van de belemmeringen waarvan Volt zegt: die belemmeringen zouden we weg moeten halen?

De heer **Dassen** (Volt):
Wat ik heb begrepen, is dat het best wel lang heeft geduurd voordat de samenwerking tussen NCC en DTC goed tot stand is gekomen. Het voorbeeld dat mevrouw Rajkowski nu noemt, is inderdaad een van de belemmeringen. Ik heb daar wel een vraag bij. Ik wil namelijk kijken hoe je kunt zorgen dat data die je hebt over cyberdreigingen zo snel mogelijk gedeeld kunnen worden. Dan moet je dus ook kijken hoe het kan dat dit soort belemmeringen op dit moment nog aanwezig zijn, of er nog meer aanwezig zijn en hoe we die kunnen weghalen.

De **voorzitter**:
Oké, dan dank ik de heer Dassen en vraag ik mevrouw Van Weerdenburg om het voorzitterschap tijdelijk over te nemen.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dat zal ik doen. Dan geef ik nu het woord aan mevrouw Leijten voor haar inbreng namens de SP.

Mevrouw **Leijten** (SP):
Als de treinen niet rijden, dan is het volledige land ontregeld en als het betaalverkeer stilligt, dan is dat een klap voor de economie. Als waterkeringen, kerncentrales of ziekenhuizen gehackt worden, dan zijn de gevolgen voor het land niet te overzien. Daarom is het van cruciaal belang dat onze digitale wereld veilig is, zodat het land kan functioneren en mensen beschermd zijn tegen criminelen die aan de haal gaan met onze gegevens.
Van de ernst hiervan zijn veel mensen wel overtuigd, maar de urgentie wordt toch nog altijd onderschat. De systemen zijn niet op orde, zo concluderen de Rekenkamer en het Nationaal Cyber Security Centrum. De Algemene Rekenkamer stelde in mei 2021 dat de stand van de informatiebeveiliging rijksbreed over de hele linie gezien in 2020 niet is veranderd. Vrijwel alle organisaties die de informatiebeveiliging in 2019 niet op orde hadden, hebben hier wel werk van gemaakt, maar dat heeft niet geleid tot voldoende beheersing van risico's, waardoor de onvolkomenheden nog niet zijn opgelost. De Cyber Security Raad constateerde dat in Nederland de komende jaren additionele inzet en investeringen nodig zijn om de weerbaarheid te versterken.
Die investeringen in de cybersecurity zijn er deels, maar volgens de SP niet voldoende. Zo zijn er het afgelopen jaar maar liefst 23.976 datalekmeldingen gedaan bij de Autoriteit Persoonsgegevens. In maart 2021 bleek dat privégegevens van mogelijk miljoenen Nederlandse autobezitters gestolen waren en te koop staan op internet. Dan gaat het om naam, adresgegevens, e-mailadressen, kentekens, telefoonnummers, geboortedata. De Autoriteit Persoonsgegevens staat onder zeer zware druk.
Nu ligt er een amendement van de SP voor bij deze begroting – we stemmen er volgende week over – voor extra investeringen, en toch presteert de Minister van Justitie en Veiligheid het om dit amendement te

ontraden. Waarom toch? Als je zelf demissionair geen besluiten wilt nemen, waarom laat je het dan niet aan de Kamer om geld te verschuiven? Erkent de Minister wel hoe hoog de druk is en hoe noodzakelijk het is dat de Autoriteit Persoonsgegevens meer middelen krijgt? Er wordt door dit kabinet geïnvesteerd om cybercriminaliteit tegen te gaan door extra rechercheurs in te zetten op dit onderwerp, maar tegelijkertijd weten we hoe hoog de druk op de politie is en dat er onvoldoende wordt geïnvesteerd in nieuwe agenten. De kans dat investeringen op dit gebied zichzelf terugverdienen, zoals ook bij financieel rechercheurs wordt gesteld, is levensgroot. Is het demissionaire kabinet dat met de SP eens? Er is weliswaar nog steeds geen inzicht in de schade die cybercriminelen berokkenen, maar schattingen lopen in de vele miljoenen en miljarden wereldwijd.
Dat we niet weten hoeveel schade het oplevert, komt onder andere doordat de meldingsbereidheid zo laag is. Dat moet anders, want we kunnen deze criminelen alleen treffen door het verdienmodel aan te pakken, te leren hoe ze werken en die ervaringen te delen. Is het kabinet bereid een meldingsplicht in te stellen voor als je slachtoffer wordt van ransomware? Dan kunnen we namelijk informatie uitwisselen en kunnen we proberen het verdienmodel aan te pakken, door bijvoorbeeld geen losgeld te betalen. Is het kabinet het met de SP eens dat we dit als norm moeten inzetten? En is het kabinet bereid om dit uit te werken?
Een verbod op losgeld voor gegijzelde data betekent wel dat bedrijven en instellingen die dit meemaken, voldoende ondersteuning moeten krijgen in hoe ze om moeten gaan met dit soort criminelen. Het Cyber Security Center schrijft daarover dat cybersecurityexperts signaleren dat er grote verschillen in weerbaarheid zijn in Nederland. Grote bedrijven kunnen investeren in kennis en kunde op dit gebied, en aanbieders van essentiële diensten en digitale dienstverleners hebben een zorgplicht, die wettelijk is vastgelegd in de Wet beveiliging netwerk- en informatiesystemen.
Kleine bedrijven daarentegen – neem bijvoorbeeld het mkb – beschikken veelal niet over die expertise en de middelen om die weerbaarheid naar een hoger plan te tillen. 46% van de ondernemers geeft aan met gijzelsoftware te maken te hebben gehad. Hoe kunnen we dit verbeteren? Hoe kunnen we bijvoorbeeld het Digital Trust Center hierin een betere rol laten spelen? Of vindt de Minister van Economische Zaken het inmiddels voldoende? Het is wat ons betreft een probleem van de hele samenleving als de privacy van mensen ernstig wordt aangetast, bijvoorbeeld door dit soort gijzelsoftware.
Wij willen er wel op wijzen dat voorkomen beter is dan genezen. De SP ziet dat dit gevoel van urgentie op veel plekken niet voldoende of afwezig is, en menselijk handelen maakt systemen kwetsbaar: zwakke wachtwoorden, geen tweetrapsverificatie, het niet uitvoeren van beveiligingsupdates. Ook dat gaat de hele samenleving aan. Nu hebben we handreikingen die worden gepubliceerd op websites, maar ik zie ons niet iedere ochtend die websites bezoeken. Waarom is er niet een grootschalige campagne, zoals we die bijvoorbeeld ook hebben voor dat je je ramen en je deuren moet sluiten als je je woning verlaat? Aan het aantal communicatiemedewerkers in dienst van de overheid kan het niet liggen dat zo'n goede publiekscampagne niet wordt ontwikkeld.
Ook toezicht is essentieel. Ik heb het al gezegd: niet alleen de Autoriteit Persoonsgegevens staat onder druk, het algehele toezicht staat onder druk, en het is ook nog eens versnipperd. Wij hebben in het verleden gepleit voor een nationale inspectie. Die zou departementoverstijgend kunnen zijn. Bijvoorbeeld op het gebied van digitale veiligheid zou dat heel veel voordelen bieden. Is het kabinet bereid dit te onderzoeken, zodat we hiermee met een volgend kabinet aan de slag kunnen?
Dank u wel.

De **voorzitter**:

Dank u wel, mevrouw Leijten. Er is een interruptie van mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Een van de punten van mevrouw Leijten, halverwege haar betoog, was dat er een meldingsplicht zou moeten komen als je slachtoffer bent van een ransomware-aanval. Ik kan me voorstellen dat dit kan helpen en dat er meer informatie en kennis gedeeld wordt over ransomware-aanvallen; hoe dan, waar dan en wanneer dan. Ik vraag me dan alleen af of dit wel de juiste route is. Uiteindelijk is deze informatie juist voor bedrijven vaak heel spannend om te delen. Zou het niet interessanter zijn om juist in te kunnen zetten op een vertrouwde omgeving waarin bedrijven dit soort informatie ook met elkaar durven te delen, in plaats van op een verplichting vanuit de overheid? Dat is dus een vraag. Wat moeten ze dan eigenlijk precies melden en wanneer?

Mevrouw **Leijten** (SP):
Ik heb met al die afkortingen zoals Trust Center en Digital Cyber Center nog niet helemaal scherp waar dat het beste zou kunnen. Het lijkt mij goed dat je het veilig kunt melden, maar dat je wel een meldplicht hebt. Het kan best zijn dat vandaag het ene bedrijf getroffen wordt door een groep die ransomware gebruikt en morgen het andere bedrijf door dezelfde groep met dezelfde ransomware. Je kunt met een meldplicht dan toch preventief aan de slag en je kunt detecteren hoe groot, of wellicht hoe krachtig, de aanval is. Daarom zou ik daar ook voor zijn.
Dat betekent niet dat het een publieke melding moet zijn en dat het meteen in de krant moet staan. Ik begrijp heel erg goed dat je dat op een veilige manier moet doen. We moeten wel de afspraak maken dat we elkaar in die preventie moeten helpen, en noem het allemaal maar op. Het is een publiek belang dat we het weten als er ergens een aanval is geweest. We moeten het ook begeleiden als gezegd wordt dat er geen losgeld wordt betaald. Je moet weten dat je meteen hulp kunt krijgen met het misschien oplossen daarvan. Ik zou er heel erg voor zijn dat we dat wel creëren. Dat kan je via zo'n meldingsplicht doen. Wat mij betreft moeten het dan wel vertrouwelijke meldingen zijn. Of we moeten het op zo'n manier inrichten dat het niet meteen op straat ligt, maar dat je dus in de boezem van een van de trustcenters snel die koppeling kunt maken, zodat je ook snel kunt handelen als het echt een hele grote aanval is die je wilt stopzetten, en dat we heel snel anderen kunnen waarschuwen voor dit soort ransomware om achterdeuren dicht te zetten. Daar is die meldplicht echt voor bedoeld.

De **voorzitter**:
Dank u wel. Er is nog een vraag van de heer Amhaouch.

De heer **Amhaouch** (CDA):
Mevrouw Leijten van de SP gaf een beetje het beeld van de versnippering aan. Zij vroeg: waar moeten we gaan versterken? Ze had het over de Autoriteit Persoonsgegevens. Wat vindt de SP, zeker in deze fase, van het idee van een nationale coördinator cybersecurity of cyberveiligheid, die het totaalplaatje heeft en die inderdaad kan beoordelen welke organisatie op welke plek versterkt moet worden? Je kunt er natuurlijk wel één organisatie uit halen, maar er zijn misschien meerdere organisaties die je in balans moet brengen ofwel in verbinding moet brengen. Hoe kijkt de SP daartegenaan?

Mevrouw **Leijten** (SP):
Ik weet dat het Digital Trust Center er in het verleden onder andere op initiatief van de Kamer is gekomen. Wij zeiden dat er een plek moet zijn waar je samen kunt komen. Ik ben een beetje huiverig voor het idee dat je

op alles wat we hebben opgetuigd nou ook weer een nationaal coördinator moet zetten om dat te coördineren. Ik snap wel de bedoeling van de vraag van het CDA. Hoe zorgen we er nou voor dat we weten waar we moeten zijn voor welke ondersteuning, bijvoorbeeld voor het inrichten van zoiets als een meldplicht waar wij voor pleiten? Ik wil eigenlijk het liefst even horen wat de Minister daarop te zeggen heeft, om eventjes in te schatten wat de beste weg is om dit te bewandelen. Maar we lopen allemaal tegen die versnippering aan. Dat hebben we ook gezien aan de afkortingen die hier in dit debat helaas niet te weinig worden gebruikt.

De **voorzitter**:
Dank u wel. Tot slot had mevrouw Kathmann ook nog een zeer beknopte vraag.

Mevrouw **Kathmann** (PvdA):
Ja, een heel beknopte. Mevrouw Rajkowski stelde deze vraag zelf aan mevrouw Leijten. Ik zou graag van mevrouw Rajkowski willen weten: ziet zij ... Dat kan niet? O!

De **voorzitter**:
Dat kan niet. De termijn van mevrouw Rajkowski is geweest.

Mevrouw **Kathmann** (PvdA):
Ik kan niets aan haar vragen over wat zij eerder aan mevrouw Leijten heeft gevraagd?

De **voorzitter**:
Nee, helaas.

Mevrouw **Kathmann** (PvdA):
Dat wist ik niet.

De **voorzitter**:
Maar u heeft ook nog een tweede termijn. Hou het vast, zou ik tegen mevrouw Kathmann willen zeggen.
Dan geef ik nu weer het voorzitterschap over aan mevrouw Leijten.

Voorzitter: Leijten

De **voorzitter**:
Deze voorzitter houdt er altijd heel erg van om creatief om te gaan met de vragen die je hebt, maar je kan echt niet in de termijn van een ander vragen stellen aan een andere fractie.
Ik had jullie beloofd om nog eventjes de afkortingen langs te lopen. CSR is Cyber Security Raad. WODC is Wetenschappelijk Onderzoek- en Documentatiecentrum. DTC is Digital Trust Center. NCSC is het Nationaal Cyber Security Centrum. NCTV is de Nationaal Coördinator Terrorisme en Veiligheid. O, het is de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Het is maar goed dat ik hier de Minister van Veiligheid en Justitie naast me heb zitten. Hij is me de hele tijd aan het verbeteren. Dan kan ik niet meer goed voorzitten.
De bewindspersonen hebben aangegeven twintig minuten schorsing nodig te hebben. Ik denk dat we daarmee ook voldoende tijd hebben om een goede eerste termijn van de zijde van de bewindspersonen te verwachten. Ik wil wel aangeven, omdat u met z'n drieën bent, dat ik ga knijpen op de belangrijke woorden van de demissionaire regering als het te lang wordt waardoor er geen tweede termijn meer mogelijk is. Ik denk dat dit, naar aanleiding van dit moment voor de schorsing, niet nodig zal zijn.

Ik dank de leden voor hun eerste termijn. We schorsen twintig minuten en dan komen we om 15.10 uur hier weer terug voor de antwoorden van de regering.

De vergadering wordt van 14.49 uur tot 15.09 uur geschorst.

De **voorzitter**:
Het is 15.09 uur. We hadden afgesproken dat we verder zouden gaan om 15.10 uur, maar we zijn allemaal al aanwezig, dus ik stel voor om te beginnen met de beantwoording door het demissionaire kabinet. Ik ga ervan uit dat de Minister van Justitie en Veiligheid ons even meeneemt in hoe de beantwoording zal verlopen. Het woord is aan de Minister van Justitie en Veiligheid.

Minister **Grapperhaus**:
Dank, voorzitter. Laat ik maar meteen met de deur in huis vallen: goed dat deze commissie er is. Digitale zaken is een belangrijk onderwerp. Ik denk dat het goed is dat de Tweede Kamer heeft gezegd: wij zorgen voor een zekere mate van grootste gemene deler. Dit betekent overigens niet dat onderwerpen van hier niet ook elders aan de orde zullen of kunnen komen. Zo sprak ik vanmorgen ook in het kader van de criminaliteitsbestrijding over ransomware, cybercrime en dergelijke zaken. Maar ik vind dat geen punt, want de digitale wereld is zo langzamerhand bijna de wortel van wat er in de werkelijke wereld gebeurt.
Een kleine anekdote. Toen ik net Minister was, kreeg ik een rapport ter goedkeuring en doorsturing aan de Kamer waarin duidelijk werd gemaakt dat heel veel voorzieningen in Nederland geen analoge terugvaloptie hebben. Bijvoorbeeld bepaalde bruggen kunnen gewoon niet meer open als de digitale apparatuur het laat afweten. Dat geeft een beetje aan hoe het geheel werkt. Toen ik vorige week bij mijn begrotingsdebat op de telefooncodes wees, was dat ook, zeg ik via u, voorzitter, tegen de heer Dassen, aan de hand van een ervaring die we een aantal jaren geleden opdeden met bedrijven die vooral in het internet of things investeerden. Dan moet u eraan denken dat u in de auto via uw iPhone thuis alvast de centrale verwarming aanzet. Dat is in deze tijden van veel regen lekker knus. Maar als de fabrikanten als fabrieksinstelling diezelfde code 0000 gebruiken, wordt het voor slechteriken ook heel makkelijk om in te breken. Dan komt u thuis en is het of ziedend koud of loeiend heet. Dat zijn twee voorbeelden waaruit blijkt dat cybersecurity eigenlijk overal zou moeten zijn, maar we daar toch nog niet helemaal aan gewend zijn.
Ik kom straks nog op het punt dat de voorzitter als woordvoerder maakte over de voorlichtingscampagnes. Ik wil u voorzichtig laten wennen aan het idee dat we twee jaar geleden wel degelijk een voorlichtingscampagne hadden die helemaal analoog aanhaakte – ik gebruik «analoog» nu in een andere zin – bij het op slot doen van je huis. We zeiden: als je een dievenklauw op je raam en een dubbel slot op je deur zet, waarom heb je dat dan niet ook op je computer? Ik denk dat die publiekscampagne zo weer opnieuw zou kunnen worden ingezet, want die bewustwording is zo ontzettend belangrijk.
Het is dus in ieder geval goed dat u deze commissie heeft. Dank voor uw uitnodiging. Wij zijn hier met drie kabinetsleden. Dat komt omdat digitalisering alle beleidsterreinen raakt en onderdeel is van vrijwel alle uitvoeringsprocessen, maar je ziet en wil toch dat elk departement op zijn eigen beleidsterrein zelf verantwoordelijk is voor de sturing op en de invulling van specifieke onderdelen van de betreffende thema's. Ook in de niet-digitale wereld wil je immers dat ieder zijn taak en verantwoordelijkheid blijft oppakken. Drie bewindspersonen coördineren binnen het kabinet het thema digitalisering. Allereerst is dat de Staatssecretaris van EZK, thans waargenomen door de Minister van EZK, op de digitale economie en de overkoepelende digitaliseringsstrategie. Vervolgens is dat

de Staatssecretaris van BZK, op het terrein van de digitale overheid. Ten slotte is dat de Minister van JenV, op cybersecurity. Dat ben ik. Nu heb ik toch wel weer een paar andere afkortingen gebruikt en toegevoegd aan de lijst.
Voorzitter. Om het leven voor u toch wat te verlichten, heb ik voor uw leden als geschenk het Cybersecurity Woordenboek. Ik kan u verzekeren dat de voorsprong waarvan u misschien denkt dat ik die heb op sommige terminologieën, als sneeuw voor de zon verdwijnt als u de komende dagen, op het moment dat er even iets saais doorkomt op Netflix of anderszins, dit boek doorneemt. Ik wil u het graag als eerste aanbieden, voorzitter, maar alle leden krijgen het. Daarbij merk ik overigens op dat er binnenkort een tweede druk van dit boek uitkomt, waarin ongetwijfeld de meest recente afkortingen en woorden ook weer zijn meegenomen. Maar het zegt wel iets dat we dit woordenboek hebben, want het is echt een nieuw eigen domein geworden. Het is alleen maar goed dat we dat goed kunnen omschrijven.
Voorzitter. De afgelopen periode heeft de noodzaak van de inzet op het verhogen van cyberweerbaarheid alleen maar verder onderstreept. Juist COVID-19 heeft ons laten zien dat digitalisering en het belang van digitale veiligheid nog groter worden. Aan de ene kant dus de digitalisering. Moet u zich voorstellen hoe wij vijftien jaar geleden met deze crisis hadden moeten omgaan, toen videoconferencing nog een kwestie was van heel veel sneeuw op het scherm met een poging om de ander te herkennen. Maar aan de andere kant dus de digitale veiligheid. Juist nu moeten we ervoor zorgen dat we, waar we zo veel digitaal doen, niet gehackt worden of geconfronteerd worden met ransomware. Ik kom daar straks nog op terug.
Voorzitter. We werken digitaal, we winkelen vaak digitaal en we ontmoeten elkaar tegenwoordig in die ellendige periodes waarin er meer beperkingen zijn ook heel veel digitaal. Kortom, het is allemaal zo verweven met elkaar: de werkelijkheid en de digitale wereld.
Voorzitter. Ik kom op een aantal concrete vragen. Ik heb een poging gedaan om ze zo veel mogelijk bij elkaar te nemen. Daarna zullen de collega's uiteraard de vragen op hun terrein beantwoorden.
Voorzitter. Ik begin met de vragen over de rapporten en de nieuwe strategie. Allereerst de aanbevelingen uit de evaluatie van de NCSA en natuurlijk het advies van de Cyber Security Raad. Ik denk dat het duidelijk is – ik heb dit net wat uitvoeriger genoemd – dat het enorme belang en de toename van digitale processen betekenen dat we een stevige aanpak moeten hebben, zowel op cybersecurity als op cybercrime. Dit betekent dat we de afgelopen tijd in dit kabinet wel degelijk hebben ingezet – op dat punt wil ik mevrouw Kathmann weerspreken – op een aantal nieuwe instrumenten en ook op investeringen in de cybersecurity. Die zijn vrij breed gegaan. Ik wil daarvoor niet uw tijd misbruiken, maar u echt verwijzen naar de periodieke rapportages die we u daarover hebben gestuurd, maar ook naar de jaarlijkse Nederlandse Cybersecurity Agenda, de NCSA. De conclusies uit de NCSA, maar ook uit de recente rapporten van RAND Europe en de Cyber Security Raad moeten worden betrokken bij het opstellen van een nieuwe strategie. U heeft mij het NK-woord – het nieuwe kabinet – nog niet horen uitspreken. Ik begrijp heel goed dat u als Kamer zegt: ja, maar wij willen verder. Dat is juist een van de redenen waarom dit kabinet ook op dit onderwerp heeft gezegd: dit is zo belangrijk; we moeten dat niet stil laten vallen en erop doorgaan. Dit betekent niettemin dat we voor de invulling van verdere middelen en dergelijke wel degelijk de coalitie zoals die nu zou kunnen gaan aantreden, de ruimte moeten geven om daarin de allerbelangrijkste keuzes te maken. Maar dit zittende kabinet, ook wel het «demissionaire kabinet» genoemd, blijft gewoon actief. U kunt ons daarop aanspreken. We blijven actief op basis van de NCSA.

Voorzitter. De vraag van mevrouw Van Weerdenburg over voldoende doorzettingsmacht bij het kabinet in het geval van een crisis ...

De **voorzitter**:
Een ogenblikje, Minister. Net voordat u begon met een nieuw antwoord riep dit een vraag op bij de heer Dassen.

De heer **Dassen** (Volt):
Dat klopt, voorzitter. Ik hoorde de Minister spreken over het belang en dat we er stevig op moeten inzetten. Tegelijkertijd zien we dat de investeringen de afgelopen jaren zijn achtergebleven bij de ambities ten tijde van de start van dit kabinet. Ik begrijp ook dat we moeten wachten op het nieuwe kabinet – het NK-woord – maar hoor de Minister ook zeggen dat het belangrijk is dat we de adviezen van bijvoorbeeld de Cyber Security Raad opvolgen en overnemen. Ik vraag me af of er in de voorbereiding van het nieuwe kabinet ambtelijk al wat technische voorbereidingen zijn om te kijken hoe die dan zo snel mogelijk uitgevoerd kunnen gaan worden.

Minister **Grapperhaus**:
Ik bedoel dat alleen maar constructief, maar ik moet de heer Dassen toch weerspreken. De ambities van die 95 miljoen per jaar zijn wel degelijk uitgevoerd. Ik wil uw commissie, voorzitter, graag goed geïnformeerd op pad helpen, dus ik wil u daar best een brief over sturen met een overzicht. Er zijn zelfs een aantal keren extra middelen ingezet, zowel incidenteel – ik zie mevrouw Rajkowski herkennend knikken – als structureel. Dat was ook nodig. Het is wel zo – ik denk dat de heer Dassen daar absoluut een punt heeft – dat we als samenleving in 2017 nog op een wat ander ambitieniveau zaten, omdat we tegen een aantal zaken ook anders aankeken. Maar we hebben sindsdien op het gebied van regelgeving, toetsingskaders en de doorzettingsmacht, waar ik zo nog op kom, wel degelijk dingen doorontwikkeld. Ook hebben we geïnvesteerd in alles wat met cyberweerbaarheid en cybersecurity te maken heeft.
Dan over het nieuwe kabinet. U begrijpt dat het staatsrechtelijk niet aan mij is om vooruit te lopen op wat daarmee zou gaan gebeuren. Dat kan niet. Het enige wat ik u zeg, is dat dit kabinet heel duidelijk door blijft gaan met het actief uitrollen van de Nationale Cybersecurity Agenda. Dat doen we op zodanige wijze dat een volgend kabinet een goedlopend programma overneemt en niet het gevoel heeft dat men stilstaat. U begrijpt dat ik hier niks kan zeggen, maar zo leggen we het natuurlijk wel neer bij het nieuwe kabinet.

De **voorzitter**:
Dat roept wel een vraag op bij de heer Amhaouch.

De heer **Amhaouch** (CDA):
Als wij het niet over het NK mogen hebben, gaan we even terugkijken, want ik neem aan dat er voorbereidend werk is gedaan. Het gaat mij om de algemene vraag, die ik ook zag terugkomen bij mijn collega's. Natuurlijk willen we ambities verhogen. We willen de middelen verhogen. Er is gesproken over technisch personeel. Maar heeft het kabinet ook nagedacht over wat haalbaar is in het kader van opschalen? We hebben het nu over de digitalisering. Het lijkt dan wel of cybersecurity iets extra's is naast de analoge, reguliere veiligheidskwestie. Hoe kijkt het kabinet aan tegen het opschalen, in prioriteit en ambitie? Wat is haalbaar? Los van alleen maar geld en middelen: wat kunnen we aan?

Minister **Grapperhaus**:
Dat is een vrij breed uitwaaierende vraag. Die zouden wij als drie collega's eigenlijk ieder voor ons eigen deel moeten beantwoorden, want daar zit

bijvoorbeeld ook de vraag bij wat de overheid in dat opzicht aankan. Daarvoor is collega Knops, de Staatssecretaris van BZK, hier aanwezig. Ik denk dat het algemene uitgangspunt is dat u in de Nationale Cybersecurity Agenda geformuleerd ziet wat de punten zijn waarop wij op het gebied van cybersecurity – ik zeg het even simpel – moeten inzetten in de komende tijd. De Cyber Security Raad heeft een advies gegeven. Ik kan er niet zoveel aan doen, maar dat advies was echt heel duidelijk aan het nieuwe kabinet gericht. Ik denk dat grote delen van dat advies aansluiten bij het actieprogramma waarmee we nu bezig zijn. Ik praat nu even vanuit mijn perspectief: kunnen we dat aan vanuit het departement dat de weerbaarheid en de cybersecurity moet borgen? Ja, ik denk dat we dat aankunnen. Ik meen dat mevrouw Rajkowski... Ik ben even kwijt wie nou precies de vraag over de opleiding opwierp, mevrouw Van Ginneken of mevrouw Rajkowski; misschien beiden, in koor. Opleiding is natuurlijk wel iets waar we enorm op moeten inzetten. Daarbij is overigens een lichtpunt dat mijn ervaring, zo blijkt ook uit onderzoek, is dat jonge mensen die over de opleidingsvaardigheden beschikken, zeer graag aan de slag gaan bij de rijksoverheid, in allerlei functies gelegen op het gebied van cybersecurity en aanverwante takken van sport.
Daarnaast zullen we de komende jaren als overheid echt wel degelijk alle zeilen moeten bijzetten op dit dossier. Want het digitale domein ontwikkelt zich. Het ontwikkelt zich mondiaal. En zoals ik vanmorgen heb gezegd over de cybercrime: het ontwikkelt zich niet alleen bij statelijke actoren, maar ook bij allerlei misdaadorganisaties. Sterker nog, sinds covid is cybercrime een businessmodel voor gewone criminelen geworden. Dus dat betekent dat we alle zeilen moeten bijzetten. En dat móéten we ook doen. Dus een volgend kabinet zal daarop aansluitend ongetwijfeld de goede beslissingen nemen om voort te zetten waar we nu als kabinet mee bezig zijn.
Voorzitter. Mevrouw Van Weerdenburg vroeg: is er nou voldoende doorzettingsmacht bij het kabinet in geval van crisis? In de eerste plaats is het natuurlijk zo dat organisaties zelf een verantwoordelijkheid hebben om systemen te beveiligen. De aanpak van het kabinet zal er dan op gericht zijn om partijen in staat te stellen om dat te doen. Als stelselverantwoordelijk Minister, ook voor de crisisstructuur, zal ik er altijd zorg voor dragen dat vitale aanbieders hun verantwoordelijkheid kunnen nemen. Dan is de samenwerking met andere departementen en toezichthouders altijd essentieel. Want als aanbieders van essentiële diensten geadviseerd zijn maatregelen te nemen en geconstateerd wordt dat er onvoldoende of geen opvolging aan wordt gegeven, dan ontstaat het risico op maatschappelijke ontwrichting. In dat geval informeer ik ook de verantwoordelijke Minister of toezichthouder van de betrokken sector, zodat iedereen in staat is om te doen wat nodig is. Daar komen we nog over te spreken naar aanleiding van het OVV-rapport. We hebben natuurlijk ook in de Citrix-crisis van twee jaar geleden, januari 2020, zeg ik uit mijn hoofd, toch nog betrekkelijk tijdig kunnen optreden.
Voorzitter. Daarmee kom ik op de vraag die hier in het verlengde van ligt. CDA, PVV en D66 vroegen: moet je nou een cyberminister of een nationaal cybercoördinator hebben?

De **voorzitter**:
Niet voordat u de vraag heeft beantwoord die mevrouw Van Weerdenburg voor u heeft.

Mevrouw **Van Weerdenburg** (PVV):
De Minister zegt dat de vitale aanbieders hun verantwoordelijkheid moeten nemen en dat de overheid hen daarbij moet ondersteunen en helpen. In dat kader heb ik een vraag over de Europese ontwerpverordening: de Digital Markets Act. We hebben daar eerder over gedebatteerd met Minister Blok. Toen kwam ter sprake dat daarin een verplichting staat

tot het toestaan van sideloaden. Denk bijvoorbeeld aan iPhones en iPads. Apple heeft daar een probleem mee, want het bedrijf kan de veiligheid dan niet meer garanderen. Daar hebben we een discussie over gehad. Hoe ziet de Minister dan die verplichting voor bijvoorbeeld Apple om sideloaden toe te staan? Dat zorgt namelijk voor een extra security issue. Ik kan dat niet rijmen met wat de Minister nu zegt.

Minister **Grapperhaus**:
De collega van EZK komt zo dadelijk terug op dat punt van het sideloaden. Maar nu kan ík weer niet helemaal rijmen dat het niet rijmt met wat ik gezegd heb. Dus mijn excuses; ik begrijp het even niet.

Mevrouw **Van Weerdenburg** (PVV):
De Minister zegt: we moeten vitale aanbieders helpen om hun verantwoordelijkheid te nemen. We hebben het over veiligheid en de aanbieder van iPhones. Ik geloof dat zo'n beetje de hele rijksoverheid met een iPhone loopt. Die aanbieder zegt dus: we kunnen de veiligheid niet garanderen als wij worden verplicht om sideloaden toe te staan op die toestellen. Dus Nederland is voor die verplichting tot sideloading in Europa. Maar tegelijkertijd zegt de Minister hier: nee, we moeten de vitale aanbieders ook wel de mogelijkheid geven om dat allemaal veilig te doen. In die zin was daar in mijn optiek een tegenstelling.

Minister **Grapperhaus**:
Ik begrijp dat dit onderdeel is geweest van de onderhandelingen, en dat dit opgelost is, maar daar komt collega Blok zo dadelijk in ieder geval op terug. In het algemeen geldt voor dit soort algemene issues inderdaad nu juist dat het NCSC daar richting de vitale aanbieders een taak voor heeft om het probleem te signaleren. Maar goed, collega Blok komt terug op de oplossing voor dit concrete geval.
Voorzitter. Er was een vraag over of een cyberminister zou moeten komen. Digitale veiligheid is een essentiële randvoorwaarde voor het slagen van de digitale transitie, dus je moet cybersecurity geborgd hebben op elk domein en in elke bestuurskamer. De verschillende betrokken departementen zijn binnen de huidige situatie vanuit hun eigen rol en verantwoordelijkheid daarmee aan de slag. Ik heb het de afgelopen vier jaar als coördinerend bewindspersoon heel erg als taak gezien – zo is het ook gelopen – om niet het werk van ze over te nemen, maar om goed te monitoren en collega's vervolgens aan te sporen of de adviseren. In die zin wordt er dus ook al op nationaal niveau gecoördineerd. Daar spelen NCTV en NCSC een belangrijke coördinerende rol.
Ik spreek over de afgelopen vier jaar en/of in een kader van een evaluatie van hoe dat loopt en zou moeten lopen. Hoe het dan wordt, daar ga ik mij nu niet over uitspreken. Ik denk wel dat we echt kunnen zien dat dat de afgelopen jaren – dat lag niet aan deze Minister, maar dat was gewoon doordat het echt goed belegd was – goed heeft gewerkt. Ik verwijs overigens in ieder geval naar het advies van de Cyber Security Raad, die nu juist pleit voor een onderraad in het kabinet voor cybersecurity, en ook naar het advies van de Wetenschappelijke Raad voor het Regeringsbeleid over artificial intelligence, die ook pleit voor een digitale onderraad. In allebei de adviezen zegt men – althans, zo heb ik ze gelezen; laat ik het zo zeggen – eigenlijk dat het echt van belang is dat je die coördinatie hebt en de zaken goed bij elkaar trekt, dat je dan nog steeds moet zorgen voor bijvoorbeeld coördinatie op cybersecurity en coördinatie op de digitale overheid. Men zegt eigenlijk: je moet het niet naar één Minister toe trekken. Voor wat het waard is. Ik wil dat toch in ieder geval onder uw aandacht gebracht hebben.

De **voorzitter**:

Dit roept vragen op. Niet in de laatste plaats bij de voorzitter zelf, maar ik begin met mevrouw Van Weerdenburg. Die meldde zich als eerste.

Mevrouw **Van Weerdenburg** (PVV):
Dank, voorzitter. Ik heb ook dat rapport van de Cyber Security Raad voor me en dat is toch wel snoeihard. Met alle respect, maar de Minister probeert ons hier gerust te stellen door te zeggen: we passen dan wel op de winkel, maar dat is niet erg want we hebben het goed geregeld. Maar alleen al deze zin: «Departementen werken nog onvoldoende samen en cruciale dreigingsinformatie wordt om diverse redenen niet gedeeld.» Zo'n verlammende cyberaanval kan morgen of volgende week zijn en dan hebben we nog geen nieuw kabinet. Kan de Minister daarop ingaan, dat er in hetzelfde rapport ook heel iets anders staat?

Minister **Grapperhaus**:
Nee, kijk. Ik heb niet gezegd dat de Cyber Security Raad ... Enkelen van u, onder wie meneer Dassen, hebben ook gezegd: het kabinet heeft zich de afgelopen vier jaar ingespannen, maar er zal in ieder geval gemeten naar hoe zaken zich ontwikkeld hebben extra inspanning moeten komen. Daar richt de Cyber Security Raad zich in zijn advies op een aantal punten op. Dat onderschrijf ik. Ik refereerde nu aan de adviezen van de WRR en de Cyber Security Raad over of je nu moet gaan centreren bij één Minister of niet. Nogmaals, dat zal op enig moment denk ik aan de orde komen bij datgene waar we het een paar keer over gehad hebben: bij de formatie van een nieuw kabinet. Ik attendeer op wat de Cyber Security Raad daarover adviseert.

Mevrouw **Kathmann** (PvdA):
Ik heb een vraag over de beantwoording over een Minister voor digitale zaken en de onderraad. Ik heb die rapporten waarin dat geadviseerd wordt ook gelezen. Ik zou graag van de Minister willen weten hoe hij dan ziet hoe de juiste investeringen voor een integrale aanpak naar die digitale zaken gaan. In mijn inleiding gaf ik aan dat ik het wel magertjes vond, het bedrag dat het demissionaire kabinet ervoor heeft uitgetrokken, gezien de urgentie en het feit dat wordt aangegeven dat het een topprioriteit is. We weten hoe het in Den Haag werkt: wie de centen heeft, heeft de macht. Dan kan je wel een ministerraad hebben, maar die is dan zonder centen. Dus waar beleggen we dan dat geld? Ik zou dat graag van u willen weten, want dan kunnen we daarop ook misschien eens een adviesje schrijven richting die formatietafel.

De **voorzitter**:
Ik heb de interrupties niet gemaximeerd, maar als ze kort en scherp zijn, dan kunnen we daarmee uit de voeten. De Minister.

Minister **Grapperhaus**:
Voorzitter. Ook daar weer, het is niet zo dat dit kabinet... Het wordt steeds geformuleerd als: hét demissionaire kabinet heeft zich ten doel gesteld. Nee, het is gewoon het kabinet dat met een regeerakkoord is gaan werken van de daarin werkende partijen. Toen dat begon, was het dus hoe dan ook een kabinet. Laat dat duidelijk zijn. Ik heb erop gewezen dat er in ieder geval voor dít departement structureel 95 miljoen voor cybersecurity is ingezet, hetgeen onverlet laat de investeringen die op het gebied van cyber en cyberweerbaarheid elders zijn gereserveerd of vrijgemaakt. Nogmaals, we komen nu in een situatie dat... Kijk, twee kabinetten geleden was de urgentie heel anders. We zijn in de loop der tijd natuurlijk gaan zien hoe cyber ongelofelijk veel meer in onze maatschappij is toegenomen en hoeveel meer we dus cybersecurity moeten hebben. Ik ga dat niet onder stoelen en banken steken, maar ik denk dat, zoals de heer

Dassen dat gewoon zei, de komende jaren de ambitie flink moet worden aangezet.

De **voorzitter**:
Nou hield ik de leden een beetje kort, maar ik stel wel vast dat zowel mevrouw Van Weerdenburg als mevrouw Kathmann een vraag stelde die niet is beantwoord. De eerste vraag was of dit kabinet wel de urgentie voelt als er volgende week iets gebeurt. En mevrouw Kathmann zei: als je nou de onderministerraad vormgeeft zonder geld, waar ligt dan het primaat? Ik zou daar nog een vraag aan toe willen voegen. Als het een onderraad wordt, kan de Minister dan een bespiegeling geven op hoe de informatiepositie van de Kamer wordt vormgegeven? Ik vraag dat, want het is niet op te vragen en niet te wobben. En dan verdwijnt het helemaal in een zwart gat.

Minister **Grapperhaus**:
Voorzitter, ik geloof dat de Kamerleden zelf moeten aangeven of ze vinden dat ze geen antwoord hebben gekregen.
Uw vraag is een terecht punt. Je gaat krijgen dat er een commissie voor digitale zaken komt. Die is er! Maar dan zijn er nog steeds heel veel onderwerpen die onderscheiden bij departementen aan de orde komen. De Wob? Daar zou ik echt met de collega van BZK over moeten nadenken. Daarna wil ik er best bij de Kamer op terugkomen. Ik heb dat niet zo bedacht, maar ik denk voor het overige dat we nou juist door de komst van deze commissie, waar ik in het begin ook iets positiefs over heb gezegd, een soort overallcontrole hebben. Die controle kan een spiegelbeeld zijn van die onderraad. Ik denk dat we zo met elkaar afspraken moeten gaan maken als... Nu begin ik me toch op een ander terrein te begeven, maar ik zou me kunnen voorstellen dat een nieuw kabinet daar met u goede afspraken over maakt.
Laat ik één ding heel duidelijk zeggen: ik ben echt blij dat we dit hebben. Ik heb hier in het verleden namelijk ook gezeten in een zaal die net zo groot was, maar waar wel heel wat minder mensen waren. Het is een wezenlijk onderwerp en het heeft echt, zeg ik tegen mevrouw Kathmann en anderen, door covid nog een gigantische extra slag gemaakt. Ransomware en dat soort dingen komen nu veel vaker voor. Dus laat ik het hier hardop uitspreken: ik vind dat dit kabinet de tijd die hem nog gegeven is, echt op alle punten met u moet gaan afspreken hoe we goed met elkaar in een gelijkmatige pas met de commissie Digitale Zaken en de ministeriële onderraad, als die er zou komen, of... Misschien komt er toch een Minister voor Digitale Zaken, want ik ben er straks niet bij als die afspraken worden gemaakt. We moeten dat goed gelijk op laten lopen.
Ik heb voorgesteld dat ik met de collega van BZK terugkom op de Wob. Dat kan ik echt niet zo gauw even beantwoorden. Dat weet ik niet.

De **voorzitter**:
U vervolgt uw betoog.

Minister **Grapperhaus**:
Voorzitter. Dan was ik gekomen bij het afschaffen van de zerodays. De politie koopt geen zerodays. Mocht de politie tijdens een onderzoek op een zeroday stuiten, dan wordt die in beginsel gemeld bij de fabrikant. Mocht een zwaarwegend opsporingsbelang zich daartegen verzetten, dan biedt Strafvordering de mogelijkheid de melding uit te stellen. Wel kan de politie, als er geen andere mogelijkheid is, in het opsporingsonderzoek onder voorwaarden binnendringingssoftware aanschaffen die mogelijk gebruikmaakt van onbekende kwetsbaarheden. Het is overigens doorgaans niet bekend of de software van zerodays gebruikmaakt, omdat de producent dat niet vermeldt. Zoals afgesproken – ik moet het even goed zeggen! – in het regeerakkoord van het thans demissionaire maar

toch nog wel even zittende kabinet koopt de politie alleen binnendringingssoftware als dat in een specifiek opsporingsonderzoek noodzakelijk is. Daar waken we ook echt voor.

De **voorzitter**:
Mevrouw Van Ginneken heeft daar een vraag over.

Mevrouw **Van Ginneken** (D66):
Laat ik eerst dankzeggen voor de mededeling dat de politie geen zerodays aanschaft. Dat is een geruststelling. Als die via software van derden alsnog aangeschaft wordt, dan blijft deze industrie natuurlijk wel gesupport worden. Dus de vraag is even of de Minister wat specifieker kan zijn over wat voor indringingssoftware er dan gekocht wordt. Misschien was de Minister verder al van plan om daarbij ook iets te zeggen over NSO en Pegasus.

Minister **Grapperhaus**:
Meteen even over Pegasus. Over het gebruik van de diensten kunnen we in het openbare debat niets zeggen. Ik weet dat mevrouw Van Ginneken daar begrip voor heeft.
Organisaties, bedrijven en burgers moeten in eerste instantie zelf de verantwoordelijkheid nemen voor de maatregelen om de digitale veiligheid te beoordelen. Ze kunnen advies krijgen van verschillende partijen en op de website van de NCTV is een overzicht te vinden van partijen en instanties die daarvoor handvatten kunnen bieden. Daarnaast heb je natuurlijk ook alle publieke informatieverstrekking om de algehele digitale weerbaarheid te verhogen. We waarschuwen – daar komen de afkortingen – in al die publicaties, het CSBN en het DBSA, tegen bijvoorbeeld spionagerisico's. Ik heb het ook niet bedacht, maar – daar komt-ie – het NCSC, het Nationaal Cybersecurity Centrum, verstrekt algemene dreigingsinformatie en informeert de rijksoverheidspartijen en de vitale aanbieders individueel over specifieke gevallen.
In de beantwoording van Kamervragen van de heer Jasper van Dijk van de SP van 13 september jongstleden hebben mijn ambtsgenoten van BZ en BZK gemeld dat de onlineveiligheid van mensenrechtenverdedigers en journalisten een prioriteit is van Nederland. Ik kan daar op dit moment niet meer over zeggen dan wat ik daarover heb gezegd.

De **voorzitter**:
Dan vervolgt u uw betoog.

Minister **Grapperhaus**:
Voorzitter. De heer Dassen vroeg of er een schatting te maken is van de maatschappelijke en economische schade van cybercrime. De Veiligheidsmonitor geeft aan dat 13% van de Nederlanders slachtoffer is geworden van cybercrime of onlinefraudevormen. 5,5% van de Nederlanders is slachtoffer geworden van een vorm van hacken. Ik ben zonder meer bereid om te zorgen dat die gegevens of in ieder geval de vindplaatsen even per omgaande nog een keer bij uw Kamer komen, want anders moet iedereen driftig meeschrijven. Dat zijn dus de Veiligheidsmonitor van 2019 en die van 2020.
Het aantal meldingen en aangiften is veel lager. Bij de politie zijn in 2020 10.770 cybercrimemisdrijven geregistreerd. Dat is ruim een verdubbeling ten opzichte van het jaar daarvoor. Het aantal opsporingsonderzoeken naar cybercrime neemt toe. Het aantal reguliere onderzoeken groeide van 381 in '19 naar 468 in '20. Het aantal grote fenomeenonderzoeken groeide van 21 naar 39. Het is niet mogelijk om een betrouwbaar cijfer te geven voor het schadebedrag. Ik weet dat sommige cybersecuritybedrijven wel schattingen publiceren, maar daar kunnen wij niet iets van bevestigen. We werken op dit moment aan een verbetering van het inzicht door

uitbreiding van de Veiligheidsmonitor op het gebied van cybercrime en onlinefraude.

De **voorzitter**:
De heer Dassen heeft daarover een vraag.

De heer **Dassen** (Volt):
Dank, Minister. U noemde helemaal in het begin de bewustwordingscampagne van twee jaar geleden. U geeft net 13% aan en ik vind dat een vrij hoog aantal. Is er effect te zien van die bewustwordingscampagne? Gaat dat cijfer omlaag of is dat verbeterd? De Minister gaf ook aan dat het goed zou zijn als daar weer een bewustzijnscampagne op volgt. Kan de Minister toezeggen dat daarmee aan de slag wordt gegaan?

Minister **Grapperhaus**:
Ik noemde dat even, omdat het mijn eer te na was om te zeggen... We hebben natuurlijk twee jaar geleden die analogie met deursloten en zo gemaakt. We werken continu aan campagnes. Ik heb een maand of twee geleden nog met het mkb op een filmpje gestaan, waarin we een nieuwe campagne voor het mkb op dat punt hebben geïnitieerd. We doen dat gericht op ouderen, maar ook inderdaad gewoon op de beveiliging van de burger. Ik zal ook in dat opzicht... Ik zeg heel veel informatie toe, maar ik wil uw commissie graag gewoon helpen. Ik zeg toe, voorzitter, dat ik naar aanleiding van de heer Dassen in de komende paar weken even een overzicht zal geven van alle campagnes van de laatste drie, vier jaar. Dan kan hij ook echt zien dat de bewustwording op zichzelf toeneemt, maar dat dit nog altijd een kwestie is die we écht bij de burger en de bedrijven goed tussen de oren moeten zien te krijgen. Ik voer ook groepsgesprekken met mkb-bedrijven, met bedrijven die al wel slachtoffer zijn geworden en bedrijven die nog geen slachtoffer zijn geworden. We praten over hun ervaringen, over wat die betekenen en op welke manier de bewustwording volgens hen verder gebracht kan worden. Het klinkt heel erg somber, maar we zijn allemaal nog steeds heel zonnig over de veiligheid van onze apparaten.

De **voorzitter**:
De Minister vervolgt zijn betoog. O, er is nog een vraag. Ik kan alle leden nog niet zo goed lezen om te zien of ze een vraag willen stellen. Ik dacht dat het knikje betekende dat het voldoende was, maar het knikje betekende: ik wil nog wat vragen. Meneer Dassen, kort alstublieft.

De heer **Dassen** (Volt):
Ik houd het kort. Ik vroeg me af hoe de cijfers in andere landen zijn en wat daar gebeurt. Wil de Minister dat misschien meenemen? Misschien komt hij daar dadelijk nog op terug, maar kan hij daarbij ook kijken naar het Cyber Security Information Sharing Partnership in het Verenigd Koninkrijk? Daar worden dit soort dreigingen realtime met elkaar gedeeld. Heeft dat effect op de cijfers?

Minister **Grapperhaus**:
Ik wil daar twee dingen over zeggen. Het zal iets langer duren, maar ik zal ook een vergelijking maken met een aantal landen. Nu ga ik wel heel veel beloven, dus mijn ambtenaren zullen mij vervloeken. Ik denk dat dat een goed punt is. We moeten ons realiseren dat het vijftien jaar gekost heeft om de bob-campagne – dat is een geheel ander onderwerp, maar dat is voor een deel ook mijn verantwoordelijkheid – bij mensen in te laten wortelen. MONO zal de meesten van u niks zeggen, maar dat is een later gestarte campagne om niet tegelijk te appen en achter het stuur te zitten. Die loopt nu iets minder dan vier jaar en je merkt dat die nog veel minder bereik heeft. Ik vrees dat dit soort campagnes heel veel tijd kosten. De

Citrixaanval van twee jaar geleden gaf een soort shockeffect, waardoor de bewustwording weer even heel erg toenam. Het is terecht dat de heer Dassen dat kritisch volgt. Dat moet hij blijven doen, maar we zullen ons met z'n allen moeten realiseren dat de overgang naar een fase waarin iedereen cyberveilig in het leven staat, echt wat tijd in beslag zal nemen. De boeven worden natuurlijk steeds beter. Voorzitter, u ik kregen drie of vier geleden nog phishingmails waar we hartelijk om moesten lachen vanwege de vele taalfouten, maar nu zijn ze bijna niet meer van echt te onderscheiden.

De **voorzitter**:
Ik stel voor dat de Minister zijn beantwoording vervolgt.

Minister **Grapperhaus**:
De collega van EZK zal hier overigens verder op ingaan. Ik ging, geloof ik, al iets te ver in de beantwoording.
Dan kom ik op de ransomwarenorm voor losgeldbetalingen. Laat ik beginnen met te zeggen dat slachtoffer worden van ransomware heel veel impact kan hebben. De schade kan enorm oplopen. Ik begrijp dat dat slachtoffers in een heel lastig dilemma plaatst. Het advies blijft om geen losgeld te betalen, want het probleem is na de betaling van het losgeld niet zonder meer voorbij. Het biedt geen garantie dat de criminelen a de systemen weer volledig toegankelijk maken en b niet toch nog verborgen aanwezig blijven. Ook als er wel losgeld is betaald, is het in veel gevallen nodig om de infrastructuur weer helemaal op te bouwen. Ook dat kost heel veel geld. Uit onderzoek blijkt dat het uitbetaalde losgeld voor een deel gewoon weer geïnvesteerd wordt door criminelen in het verder verfijnen van hun systemen. Ik heb niet gezegd dat ik dit per se wil. Ik heb hier juist advies over gevraagd, want ik heb gehoord dat sommige verzekeringsmaatschappijen en anderen zeggen: doe dat maar wel, want dat kost minder. Ik hoop dat het voortschrijdend inzicht waarom is gevraagd, wederzijds is, aan de kant van uw Kamer en aan de kant van de verzekeraars. We moeten even doordenken. Als we dat ransomwaregedoe zo veel mogelijk willen temmen, dan is het allerbelangrijkste dat iedereen zijn systemen met optimale digitale dijkbewaking zo veilig mogelijk houdt. Dat is het eerste.
Het tweede is dat iedereen zo veel mogelijk moet melden wat er gebeurt. Daarmee kan ik meteen de vraag van mevrouw Rajkowski beantwoorden. Dan heb ik die meteen gehad. Dat geldt al voor de vitale sectoren. We kijken nu naar uitbreiding van die groep. Dan kunnen we met uw Kamer, met uw commissie discussiëren over hoever we vinden dat dit moet gaan. Nogmaals, de discussie is nog niet beslecht, maar ik geef ook wat voedsel voor het denken; excuus voor het anglicisme. Je moet ook even de andere kant op redeneren, want we moeten hiervan afkomen. Dat doen we uiteindelijk misschien toch alleen maar door de kiezen op elkaar te zetten. Als je je digitale dijkbewaking op orde hebt, zou je veel minder schade moeten hebben van ransomware, als je al schade hebt. Ik deel wat de heer Amhaouch en mevrouw Leijten zeggen: het is niet zwart-wit. We moeten echt alle nuances heel goed met elkaar gaan bekijken. We hebben gewoon te maken met geavanceerde, internationaal georganiseerde cybercriminele groeperingen. Houd er dus rekening mee dat die niet door één keer betalen voorgoed van het bord zijn.
Voorzitter. Mevrouw Rajkowski had een vraag over het delen van informatie over ransomwaredreigingen en -besmettingen. Het NCSC heeft primair de taak om vitale aanbieders en de rijksoverheid proactief te informeren over digitale dreigingen. Men deelt ook informatie over de relevante dreigingen en incidenten via de aangewezen schakelorganisaties, u welbekend, in het landelijk dekkend stelsel. Men werkt ook samen met vitale en niet-vitale organisaties die kunnen bijdragen aan het versterken van het actuele beeld, onder andere door kennis hierover met

elkaar uit te wisselen. Verder zal mijn collega kunnen ingaan op de rol die het Digital Trust Center daarbij speelt.

De **voorzitter**:
Ik geef mevrouw Rajkowski het woord voor een vraag.

Mevrouw **Rajkowski** (VVD):
Toch nog even over dat losgeld, want het zal je maar gebeuren dat je je hele leven hebt gewerkt aan het opbouwen van een mooi bedrijf, dat jouw bedrijf wordt gegijzeld en de enige uitweg die je misschien zelf ziet het betalen van losgeld is. Ik ben het eens met de Minister dat losgeld betalen nooit een goed idee is. Alleen, wanneer we tegen een ondernemer in deze situatie zeggen «maar u mag het ook niet betalen», dan gaan we wel een situatie creëren waarin een ondernemer eigenlijk geen kant meer op kan. Ik zou eigenlijk veel liever zien dat de samenwerking om te voorkomen dat er überhaupt losgeld betaald moet worden, aan de voorkant wordt ingestoken. Als verzekeraars ook zo graag willen dat hun bedrijven niet gegijzeld worden, dan kunnen zij ook eisen stellen aan het bedrijf waarmee zij samenwerken. Deze verantwoordelijkheid ligt dus ook echt op meerdere terreinen, maar laten we ondernemers die zo in de knel zitten alsjeblieft geen rijksoverheid laten zien die tegenwerkt.

Minister **Grapperhaus**:
Ik heb heel veel waardering voor een groot aantal punten die mevrouw Rajkowski aan de orde stelt, maar ik vrees toch dat we de discussie dan nu al aan de voorkant, in de vijfde minuut, willen beslechten, dat we van het veld lopen en zeggen: oké, we doen het niet. Dat moeten we niet doen. Je kunt erover nadenken dat je je er wel voor mag verzekeren dat je geen losgeld betaalt. Dat is een interessante gedachte. Als je je digitale dijkbewaking zo goed op orde brengt, dan zou in beginsel de premie voor het niet hoeven betalen van losgeld maar het weer op orde brengen van je systemen weleens lager kunnen uitpakken. Maar dat gaat het niet worden als we al in de beginminuten van de wedstrijd zeggen: we moeten beslist geen verbod doen. Ik heb heel veel sympathie voor ondernemers. Dat weet mevrouw Rajkowski. Ik ben er zelf gedurende 27 jaar ook een geweest. Ik weet hoe lastig het is om op enig moment geconfronteerd te worden met niet voorziene, en soms ook wel voorziene, al of niet verzekerde schades. Maar we moeten onszelf echt realiseren dat er een dreiging in onze maatschappij aan het komen is die we vijf jaar geleden onszelf nog niet hadden kunnen voorstellen. Ik roep het bij u in herinnering. In 2017 hadden we twee ziekenhuizen in Groot-Brittannië die platgingen. We hadden de terminal in Rotterdam. Ik noem er maar even een paar. Je moet er niet aan denken dat we dat soort dingen in de toekomst nog meer krijgen. We moeten dus hoe dan ook de digitale dijkbewaking op orde krijgen. Ik wil jegens mevrouw Rajkowski heel duidelijk stipuleren dat het mij niet per se om het ene of het andere gaat. Ik vind dat we moeten kiezen voor een oplossing die de cybersecurity maximaal maakt en daarmee ondernemers uiteindelijk ook beschermt. Laten we dat debat hier de komende tijd voeren. Ik heb er ook een onderzoek over gevraagd, want ik heb daarover niet de wijsheid in pacht.

De **voorzitter**:
Mevrouw Van Ginneken had zich ook gemeld. Is dat nog steeds nodig?

Mevrouw **Van Ginneken** (D66):
Ja, voorzitter. U zag terecht enige aarzeling, maar ik stel mijn vraag dan toch maar. Ik wil me aansluiten bij het pleidooi van mevrouw Rajkowski. Als bedrijven en kennisinstellingen helemaal in de hoek geduwd worden door een ransomwareaanval, zou het wel heel zuur zijn als zij door een verbod geen losgeld mogen betalen. Ik ben het helemaal met de Minister

eens dat het advies moet zijn om dat vooral niet te doen, maar ik hoor de Minister ook zeggen: als de digitale dijkbewaking op orde is komen er strengere eisen. Mijn vraag aan de Minister, die volgens mij stelselverantwoordelijke is, is dan: hoe ver zijn we daarvan verwijderd? Wanneer is het moment daar dat we als samenleving zeggen: we hebben de dijkbewaking op orde en we mogen nu ook strengere eisen gaan stellen aan bedrijven en kennisinstellingen?

Minister **Grapperhaus**:
De Wetenschappelijke Raad voor het Regeringsbeleid heeft, zoals wellicht bekend, in zijn grote advies van de zomer van 2019 gezegd dat het niet de vraag is óf er een keer een grote digitale cybersecurityramp gaat gebeuren. De vraag is alleen maar wanneer. Ik moet toegeven dat ik weliswaar geprobeerd heb om dat rapport met megafoons en andere middelen onder de aandacht te brengen, maar het werd pas echt actueel toen we de problematiek met Citrix hadden. U ziet dat het weer terugkeert. Ik denk dat door alle instanties, met name door het NCSC – straks komt een collega nog te spreken over het DTC en andere instanties – echt keihard wordt gewerkt om die risico's zo goed mogelijk te mitigeren. Maar we zullen dat ook van de kant van burgers en bedrijven zelf moeten zien, want uiteindelijk is het opzetten van een botnet nog steeds betrekkelijk eenvoudig mogelijk. Daarbij vertrouw ik er even op dat eenieder weet wat dat voor fenomeen is. Dat zijn dreigingen waar we vanuit het NCSC en de NCTV natuurlijk enorm op inzetten. Maar we moeten ons wel realiseren dat het altijd een kwestie is – dat zeggen in ieder geval allerlei deskundigen tegen ons – die je waarschijnlijk nooit naar nul kan brengen. Daarom heb ik het steeds over continue digitale dijkbewaking. Je moet je systemen dus voortdurend op die dingen blijven testen. Nogmaals, met betrekking tot de discussie over losgeld en ramsomware roep ik uw Kamer alleen maar op om kritisch met elkaar te kijken hoe we dat nou gaan oplossen de komende tijd. Ik weet zeker dat we dat ook heel goed en kritisch gaan doen.
Voorzitter. De Autoriteit ...

De **voorzitter**:
De heer Amhaouch heeft ook nog een vraag. Is die nog nodig, meneer Amhaouch?

De heer **Amhaouch** (CDA):
Ja, voorzitter. Ik zal het kort houden. Goed dat de Minister het speelveld openhoudt, om in NK-termen te spreken, en dat hij de losgeldbetaling niet direct van tafel veegt, maar wel dat onderzoek wil instellen. Ik denk dat dat heel goed is. Ik heb daarbij twee vragen. Komt het onderzoek dan ook met concrete alternatieven? Als het ene niet werkt, wat zijn dan de opties die wel zouden kunnen? Praten we dan niet alleen óver de ondernemers – zeg ik in de richting van de Minister van Economische Zaken – maar ook met de ondernemers, zodat de alternatieven ook uitvoerbaar zijn en gedragen worden? Volgens mij is deze opgave namelijk zo groot dat we die samen moeten aanpakken.

Minister **Grapperhaus**:
Ik ga ervan uit dat de collega van EZK daar nog op in zal gaan. Vanuit JenV, weer een andere afkorting, is het natuurlijk heel logisch dat je iedereen bij een consultatie betrekt.
Voorzitter. Over de Autoriteit Persoonsgegevens is door u als lid, mevrouw Leijten, gevraagd hoe het nou zit met meer investeringen en dergelijke. Ik wil wel voor de Handelingen even heel duidelijk hebben dat de appreciatie van de amendementen gedaan is door mijn collega, de Minister voor Rechtsbescherming. Dat betekent niet dat ik er niet voor sta, maar ik wil er zeker van zijn dat we daar geen misverstand over hebben.

De AP ontvangt vanaf volgend jaar structureel 6 miljoen euro extra per jaar. Er is een onafhankelijk onderzoek van KPMG waarin verschillende toekomstscenario's voor de AP worden besproken. Daarbij zitten er allerlei variëteiten in dat budget. Daarvan vind ik echt – daar ga ik toch weer de letters N en K gebruiken – dat het voor een nieuw kabinet is om daar de komende tijd over te beslissen. Maar in mijn demissionaire begroting is die 6 miljoen in ieder geval structureel opgenomen. Als de Kamer zou zeggen dat dat amendement moet worden aangenomen en dat dat nog veel meer moet zijn, dan moeten we een streep door andere dingen zetten. Overigens wil ik het belang van de toetsing door de AP hier wel benadrukken. Anders klinkt dat alsof ... Maar ik geloof dat daar geen twijfel over bestaat.
Dan nog heel kort. Mevrouw Van Ginneken roerde even iets aan over online content en schadelijke online content. Het is misschien goed om te zeggen dat hoewel de relatie tussen enerzijds de internetprovider, het platform of de host en anderzijds de gebruiker civielrechtelijk is, de overheid en mijn ministerie in het bijzonder wel een aanvullende rol ziet weggelegd in het tegengaan van illegale content. Die gaat het verst bij evident strafbare content. Dan moet u denken aan terroristische online inhoud. Daar is ook een richtlijn over in Europees verband. Dat is ook schadelijke content. Dat geldt ook voor seksueel kindermisbruik. Dat heb ik zelf nog heftig aangezwengeld in Europees verband. We werken inmiddels met een meerderheid van uw Kamer achter ons toe naar een separate autoriteit voor die twee vormen. Ten slotte wil ik nog melden dat we op grond van de motie van het Kamerlid Michon van de VVD, door mij zeer ondersteund, ook een wetsvoorstel hebben voorbereid over doxing. Je zou kunnen zeggen dat dat een vorm is van vrijheid van meningsuiting, maar ik zie dat heel anders. Ik vind – daar ben ik heel simpel over, dat is een makkelijk regeltje – dat wat je offline niet mag, ook online niet mag. We moeten dat echt de komende jaren – misschien is dat ook een campagne van vijftien jaar – goed in de maatschappij verankeren.
Dan kom ik op de samenwerking tussen het DTC en het NCSC. Daar gaat de collega het nodige over zeggen. Die werken in elke geval goed en nauw samen aan het gezamenlijke doel: het verhogen van de digitale weerbaarheid. Ze hebben onderscheiden doelgroepen: het NCSC de vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid en het DTC het niet-vitale Nederlandse bedrijfsleven. Ik denk dat het goed is dat je die twee wel naast elkaar hebt staan, omdat ze allebei een heel verschillend statuut hebben. In ieder geval is het DTC om onderling informatie uit te kunnen wisselen onlangs als een OKTT aangewezen. Ook heeft de Staatssecretaris van EZK het wetvoorstel Bevordering digitale weerbaarheid, om de juridische basis van het DTC te verstevigen – ik denk dat collega Blok daar iets over kan zeggen – in procedure gebracht. Ikzelf heb een voorstel tot wijziging van de Wbni in procedure gebracht. De Wbni was in de volksmond de cybersecuritywet, voor degenen die denken: deze afkorting is ook weer nieuw.
Ik denk dat ik genoeg heb gezegd – ik kijk even naar de heer Amhaouch – over de verplichte verzekeringen en dergelijke op het gebied van cyber.
Dan kom ik op ISIDOOR, een treffende benaming voor een cybersecurity-oefening. Kan er structureel geoefend worden? Ja, zeg ik via de voorzitter tegen mevrouw Rajkowski, dat gebeurt dus inmiddels en we zeggen dat we dat vaker moeten gaan doen. Het was ongelukkig dat door covid de oorspronkelijke editie van ISIDOOR voor 2020 is verdaagd, maar die is in ieder geval dit jaar doorgegaan. Het is een heel complexe oefening, waarvoor meerjarig veel capaciteit en voorbereidingstijd nodig is. Daarbij is juist het opwerktraject zeer belangrijk om de samenwerking te verbeteren en de leercyclus na een oefening. Je moet voor ISIDOOR dus een hele cyclus inzetten.
Mevrouw Van Ginneken vroeg of we daar meer bedrijven, private bedrijven, bij kunnen betrekken en of we jaarlijks kunnen oefenen. Een

groot deel van de deelnemers van de afgelopen ISIDOOR was al afkomstig uit de private sector. Het is een brede cross-sectorale oefening. Ik wil een volgend editie niet nu al toespitsen op enkele actoren. We moeten gewoon kijken naar een goede balans tussen publiek en privaat. In een volgend kabinet moet echt worden gekeken wanneer precies de volgende editie is. Ik heb al wat gezegd over de voorbereiding. Een jaarlijkse cyclus zou voor ISIDOOR te kort zijn, maar een tweejaarlijkse cyclus zou misschien wel goed zijn en ik denk dat die zo snel mogelijk moet worden opgestart.
Voorzitter. Dan hadden we het punt van de opleiding. Ik zei er al iets over in het begin. We hebben de afgelopen twee jaar via diverse impulsen de cybersecuritykennisontwikkeling in Nederland versterkt en dat blijven we doen, ook door in het kader van het tweede spoor van de Nationale Wetenschapsagenda door verschillende departementen gezamenlijk circa 10 miljoen vrij te laten maken voor cybersecurityonderzoek. Eerder heeft ook de Cyber Security Raad geadviseerd om meer aandacht te geven aan digitale geletterdheid in het onderwijs. Zoals ook al is aangegeven in de voortgangsrapportage van de NCSA van dit jaar, zal daar bij de herziening van het curriculum voor het basisonderwijs en dat voor de onderbouw van het voortgezet onderwijs aandacht naar uitgaan. Ik zie het hier niet in de tekst staan, maar vanmorgen heb een minuutje of tien van gedachten gewisseld over het digitale rijbewijs op de basisscholen. Zo zie je maar.
Voorzitter, dan nog Schiphol. De heer Amhaouch en ook anderen hadden daar kritische vragen over. Recentelijk, in de brief van 19 november, is uw Kamer vertrouwelijk geïnformeerd over de achtergrond en de uitdagingen van de vertraagde voortgang van de implementatie van de aanbevelingen van de Algemene Rekenkamer. De belangrijkste conclusie is in ieder geval dat het kabinet ervoor kiest om in te zetten op de voorziene eigenaarsconstructie. De overdracht wordt op dit moment nog nader uitgewerkt. Er moet echt zorg voor worden gedragen dat de cybersecurity effectief gewaarborgd wordt. Ik wil namens mijn collega, Staatssecretaris Broekers-Knol, benadrukken dat JenV en de betrokken stakeholders heel gecommitteerd zijn en blijven aan het zo spoedig mogelijk implementeren van de aanbevelingen. Uw Kamer zal medio 2022 uitvoerig nader bericht krijgen over de voortgang van de implementatie. Daarbij zal ook worden ingegaan op de vraag die u, voorzitter, als lid had over de zogenaamde stippenrapportage.
Tot zover.

De **voorzitter**:
«Medio 2022» is wel heel erg medio. Kunt u iets meer aangeven?

Minister **Grapperhaus**:
Voor het zomerreces.

De **voorzitter**:
Voor het zomerreces.

Minister **Grapperhaus**:
Uiterlijk juno 2022.
Voorzitter. Dan kom ik op deepfake. Mevrouw Rajkowski vroeg: is onze wetgeving klaar als het gaat om desinformatie, deepfake en dergelijke? Vorig jaar heeft het Rathenau Instituut in opdracht van BZK een onderzoek gedaan naar digitale dreigingen voor de democratie. Deepfakes kwamen uit het onderzoek naar voren als een van de grootste uitdagingen. Het kabinet is in ieder geval voorstander van meer transparantie over het gebruik. Dat wordt ook verplicht in de conceptverordening over artificial intelligence die nu voorligt in Brussel. Dit is typisch een voorbeeld dat je echt in Europees verband moet zien te organiseren. Strafbare content met deepfakes, zoals strafbare pornografie, is strafbaar. Nog even los van dat

het deepfake is: het is gewoon strafbare content. Ik hoop eerlijk gezegd dat we met het wetsvoorstel over doxing ook weer wat stappen kunnen zetten op dat punt. De universiteit Tilburg verricht in opdracht van het WODC op dit moment onderzoek naar de volledigheid van het juridische kader omtrent deepfakes. We kijken daarbij naar het strafrecht en het gegevensbeschermingsrecht.

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

Mevrouw **Rajkowski** (VVD):
Ik mis het auteursrecht, maar daar kom ik later nog wel op terug. Het jammere aan de Europese AI-verordening is dat de technologie voor deepfakes niet als een hoogrisicotechnologie wordt aangemerkt. Daar zit wat mij betreft een hiaat.

Minister **Grapperhaus**:
Ik vind dat een goed punt. Mag ik daar in de tweede termijn op terugkomen? Mevrouw Rajkowski heeft zo'n goed punt dat ik daar niet direct een antwoord op heb.

De **voorzitter**:
Het was niet eens een vraag, maar het is een goed punt. In de tweede termijn komt u daarop terug. U vervolgt uw betoog.

Minister **Grapperhaus**:
Voorzitter. Wanneer komt het rapport over Citrix? Kan dat sneller? Ik keek zelf ook uit naar die OVV-publicatie, maar u begrijpt dat ik niet over de planning van de OVV ga. Zodra ik ook maar even op de telefoon naar het voorkeursnummer van de OVV wijs, denk ik dat dat tot veel onrust leidt, want zij moeten dat in alle onafhankelijkheid kunnen doen. Ik heb er vertrouwen in dat dat snel zal gaan. U weet dat ik destijds hoe dan ook de opdracht heb gegeven tot een evaluatie door het COT – weer een afkorting. Die is in maart 2020 naar de Kamer gestuurd. Toen hebben we ook een aantal verbeteringen in het stelsel doorgevoerd. Deze discussie horend zal de OVV zich realiseren dat uw Kamer zeer geïnteresseerd is in een spoedige lezing van het rapport
Dan kom ik op het punt dat mevrouw Kathmann aanroerde over encryptie. Voor de toegang tot versleutelde informatie bestaan alternatieven, bijvoorbeeld binnendringen in een geautomatiseerd werk, hacken, of de opname van vertrouwelijke communicatie. Dat zijn bevoegdheden die veel capaciteit, expertise en tijd vragen. Ze hebben ook hun eigen beperkingen en er gelden soms strikte voorwaarden. Je kunt eraan twijfelen of die bevoegdheden een volwaardig alternatief zijn. Er lopen op dit moment verschillende trajecten, zoals het WODC-onderzoek naar de impact van encryptie op de opsporing en de inventarisatie door de Europese Unie naar de mogelijkheden voor toegang tot versleuteld bewijs. U heeft gezien dat in dezelfde tijd waarin deze discussie in Nederland niet verder kwam, vanuit de Europese Commissie is gezegd: we willen toch onderzoeken of er een vorm van zeer beperkte begrensde ontsleuteling mogelijk is, na toestemming van een onafhankelijke instantie als een rechter. Hoewel ik daar, zoals iedereen weet, best ideeën over heb, heb ik vanaf dat moment gezegd: ik wacht dat even af.

Mevrouw **Van Ginneken** (D66):
Ik voel de behoefte om te reageren op het punt van de encryptie. Ik hoor bij de Minister toch een soort opening om misschien wel achterdeuren – ik formuleer het maar even simpel – in encryptie te gaan creëren. Ik wil nogmaals benadrukken dat er wat mij betreft geen veilige achterdeuren zijn. Die worden namelijk ook gebruikt door partijen voor wie ze niet

bedoeld zijn. Door dit soort achterdeuren te creëren, bedreigt u volgens mij onze kenniseconomie en de veiligheid van journalisten en activisten. Ik vraag me af wat de Minister vindt van het Duits regeerakkoord. Daarin heeft de Duitse regering gezegd dat encryptie een recht is.

Minister **Grapperhaus**:
Dat heeft het huidige, demissionaire kabinet, toen het nog gewoon het kabinet was zonder dat voorvoegsel, ook gezegd naar aanleiding van een verklaring van het kabinet-Rutte II van volgens mij december 2016. Maar het gaat niet om het recht op encryptie. De vraag is – en daar zit het moeilijke discussiepunt – of je in die situaties waarin er sprake is van zware criminaliteit, om het maar even simpel te omschrijven, met een rechterlijke toetsing vooraf enigerlei zeer beperkte, tijdelijke vormen van encryptie zou moeten hebben. Dat is de vraag. Ik ken de stellige bezwaren van tegenstanders daarvan. Dat is in ieder geval voor mij mede aanleiding geweest om, toen de Europese Commissie aangaf «wij willen hier zelf verder naar kijken», te zeggen: laten we dat eerst maar eens afwachten. Dat is hoe deze Minister er op dit moment tegenaan kijkt.
Daarbij signaleer ik heel eerlijk gezegd wel het volgende. Ik heb dat vanmorgen gezegd en zeg het vanmiddag weer. Ik ben net als mevrouw Van Ginneken enorm voor de privacy van de gewone burger. Die moet gewoon niet op enigerlei wijze door de overheid bekeken worden. Sterker nog, er moeten altijd enorme waarborgen zijn om verschrikkelijke ongelukken voorkomen, die we de afgelopen jaren hebben zien gebeuren. Maar ik zet daar wel tegenover dat privacy niet het schild mag worden voor criminelen. Dat is zo langzamerhand wel iets wat heel erg begint te knarsen. Daar heb ik op dit moment de oplossing niet voor. Daarom zeg ik ook hiervan: laten we daar met uw commissie en het kabinet – zo noem ik het maar even, want het kabinet is ook een voortgaand fenomeen – het gesprek over blijven voeren. Ik wil niet dat we over een jaar tegen elkaar moeten zeggen: nu hebben we de zware criminaliteit heel erg laten gaan.
Nog één ding, voorzitter, dan ga ik door naar het volgende. Ik moedig vaak de leden van de andere commissie – maar ik wil het ook bij deze commissie doen – aan tot werkbezoeken. Nou is het NCMEC, het National Center for Missing & Exploited Children in Washington DC, misschien iets te ambitieus. Maar ik zou toch altijd nog heel graag een bezoek willen aanraden aan een van de afdelingen van de politie die zich gericht bezighouden met het bestrijden van kindermisbruik en kinderporno via het internet. Dat heeft mij enorm veel inzichten gegeven in hoe heel dringend en indringend die problematiek is. Daarmee zeg ik niet: we moeten alles opzijzetten. Maar dan begrijpt u als commissie ook wat meer van de dilemma's die in elk geval deze Minister de afgelopen jaren bezig hebben gehouden.
Dat was genoeg daarover. Over de meldplicht voor bedrijven die slachtoffer zijn van cybercrime heb ik volgens mij via mevrouw Rajkowski al iets gezegd. Dat speelt nu al bij die vitale aanbieders. We zijn dus bezig om te bekijken of we die groep kunnen uitbreiden. Ik denk dat we daar moeten bekijken of je die meldplicht verder zou moeten uitbreiden. Hoe dat zou moeten lopen, lijkt me een goed punt van discussie tussen uw Kamer en het kabinet.
Dan is er de Joint Cyber Unit, waar de heer Dassen naar vroeg. Bij deze EU-samenwerking is een belangrijk uitgangspunt van het kabinet dat die JCU gebaseerd zal zijn op vrijwillige bijdrage van de lidstaten, mede met het oog op de exclusieve bevoegdheid van lidstaten voor de nationale veiligheid: artikel 4, lid 2 van het verdrag. Daarnaast is het kabinet van mening dat samenwerking en informatie-uitwisseling het meest effectief is als er sprake is van onderling vertrouwen. Dat kun je moeilijk afdwingen door verplichte deelname aan de JCU. Voorzitter, ik zeg via u tegen de heer Dassen: ik heb dat inmiddels in de praktijk ook gezien bij het Europees Openbaar Ministerie – waar Nederland trouwens aanvankelijk

niet aan meedeed, maar nu gelukkig wel – waarbij ik zie dat dat toch een veel beter, groter draagvlak veroorzaakt.
Voorzitter. Ik heb nog een paar dingetjes. Over de Duitse strategie heb ik volgens mij al het een en ander gezegd. Ik vind overigens dat wat het nieuwe Duitse kabinet zegt, zeker aanknopingspunten bevat ter inspiratie voor de komende jaren. Laat ik dat maar even hardop gezegd hebben.
De rol die Clearing House wil spelen, past binnen de ambitie die het kabinet heeft om te komen tot een landelijk dekkend stelsel van cybersecurity in samenwerkingsverband. We zijn ook in gesprek met de initiatiefnemers om te bekijken op welke wijze dit kan worden opgenomen in het landelijk dekkende stelsel.
Voorzitter. Ik kom op het wetsvoorstel, de AP en het kunnen delen van IP-adressen met het NCSC en het DTC. We gaan krachtens de Wbni die privacy-informatie verstrekken, als dat mag, aan schakelorganisaties. Nu kan dat niet. Daarom hebben we dat wijzigingsvoorstel in procedure gebracht. We moeten bekijken hoe we het advies van de AP over dat wetsvoorstel daarin goed kunnen verwerken. Daar zit urgentie op, dus ik hoop dat we daar spoedig voortgang op kunnen boeken.
Voorzitter. Ik denk dat alles zo gezegd is. Ik sluit af met de mededeling dat ik het zeer waardeer dat we voortaan op deze wijze met een nieuwe commissie hierover – ik zou bijna willen zeggen «gecoördineerd» – van gedachten kunnen wisselen.

De **voorzitter**:
Ik geef het woord aan de Minister van Economische Zaken en Klimaat. Ik zou graag willen dat u schematisch iets aangeeft van wat u gaat behandelen. Als er dan vragen tussendoor zijn, kan ik inschatten of die meteen gesteld kunnen worden of daarna, in het kader van de voortgang van het debat.

Minister **Blok**:
Dank u wel, voorzitter. De indeling zal heel simpel op basis van sprekersvolgorde zijn, maar ik zal eerst een aantal algemene opmerkingen maken over de rol van het Ministerie van Economische Zaken en Klimaat en daarbinnen het DTC, het Digital Trust Centre, dat specifiek bedrijven ondersteunt bij cyberveiligheid. Dat brengt mij meteen op een vraag die een aantal Kamerleden stelden: hoe zorg je ervoor dat wat de overheid doet overzichtelijk blijft voor ondernemers, voor het publiek? Dit is eigenlijk een klassieke vraag, zeker in het veiligheidsdomein waar cybersecurity een steeds groter en belangrijker onderdeel van wordt. Het is onvermijdelijk dat je een aantal heel generieke onderwerpen hebt. Alles wat maar in de buurt komt van strafbaarheid en criminaliteit, ligt natuurlijk eerst op het terrein van de collega van Justitie en Veiligheid. Maar het is onvermijdelijk dat je dat verder vertaalt naar het bedrijfsleven – dan kom je bij mij terecht – en naar de overheid zelf, waarmee je bij collega Knops terechtkomt.
Neem een van de voorbeelden die aan de orde was: stel dat er een hack zou zijn op de bediening van bruggen en dat dan ook niet meer lukt in Nederland. Soms kom je ook bij een andere vakminister terecht. Maar laat ik het niet ingewikkelder maken dan de drie hier vertegenwoordigde ministeries. We werken uitstekend samen. We realiseren ons dat het een opgave is om dat overzichtelijk te houden richting het publiek en in mijn geval specifiek richting ondernemers.
Maar dan komt er een tweede aanvliegroute bij: de maatvoering van het overheidsoptreden. Die is natuurlijk altijd gekoppeld aan de mate van risico's. Collega Grapperhaus gebruikte al het oeroude, zou ik haast willen zeggen, grondbeginsel: wat offline geldt, geldt online ook. Dat geldt ook in de maatvoering van de ondersteuning, maar soms ook qua regelgeving op het gebied van ondernemers. Iedere vergelijking is kwetsbaar, maar ik ga er toch even één maken. Een heel klassieke bedreiging is brandvei-

ligheid. Daarbij doen we voor de kleine ondernemer en de particulier voorlichtingscampagnes, waarin we ze aanraden om rookmelders op te hangen. Maar als het wat groter wordt, zijn er dringende voorschriften en komt de brandweer inspecteren of er voldoende brandtrappen zijn. Als het nog groter is, zijn er maatwerkafspraken met de brandweer. En als het nóg groter is, moet je je eigen brandweer hebben. Op het gebied van cybersecurity is dat in zekere mate vergelijkbaar. We hebben inderdaad zeer gerichte campagnes, zowel gericht op het publiek als specifiek op ondernemers. Heel recent was dat «Doe je updates», om te voorkomen dat er kwetsbaarheden zijn voor hackers. Een campagne die ook al lang loopt, is «Eerst checken dan klikken», over phishingmails. Een voorlichtingscampagne is altijd een permanente opgave. De heer Dassen vroeg daar ook naar: wanneer is dat nou voldoende? Ik denk dat het eerlijke antwoord is: nooit, omdat er altijd weer nieuwe dreigingen zijn of omdat het bewustzijn verslapt. Wij doen dat in ieder geval gezamenlijk. Het lijkt mij voor burgers en ondernemers totaal irrelevant welk ministerie het doet. Wij doen dat. Voorlichting is eigenlijk je eerste verdedigingslijn.
Een tweede is: kennisdeling en kennisontwikkeling. Daarin speelt het DTC een grote rol. De heer Amhaouch vroeg ook: worden bedrijven daarin betrokken? Nou, heel nadrukkelijk. Dat wordt ook gewaardeerd. Een recent voorbeeld was VDL. Dat werd zelf geconfronteerd met zo'n hack. Dan hebben wij daar nauw contact mee. Toevallig zou ik daar langsgaan op de dag waarop dat bekend werd. Dat heb ik toen maar een weekje uitgesteld. Daarna ben ik toch gegaan. Dan zie je de waardering voor het delen van kennis, maar ook de verantwoordelijkheidsverdeling: zij nemen allereerst direct zelf maatregelen. Ze informeerden hun leveranciers. Maar ze informeerden ons ook over wat ervan te leren valt en hoe voorkomen kan worden dat collega-bedrijven ook het slachtoffer worden. Dat is kennisdeling.
Nadrukkelijk hoort daar ook bij: kennisontwikkeling. Onder verantwoordelijkheid van mijn ministerie valt daar nadrukkelijk onder: dcypher. Dat is een platform waarop bedrijven die hier zeer bij betrokken zijn maar ook kennisinstellingen en wetenschappers om tafel zitten over de vraag wat ontwikkelingen, bijvoorbeeld rond artificial intelligence of kwantumcomputers, kunnen gaan betekenen op het gebied van cybersecurity. Die kennisontwikkeling is dus een nadrukkelijk onderdeel daarvan.
Onvermijdelijk in de overheidsgereedschapskist met betrekking tot ondernemers is ook het onderdeel regulering. Daar heb ik in ieder geval met een deel van uw commissie regelmatig over gesproken, omdat dat vaak en wat mij betreft ook bij voorkeur Europese regels zijn. Dit is namelijk bij uitstek grensoverschrijdend. Er is dus een Europese Cybersecurity Act. Die bestaat al. De implementatiewetgeving ligt volgens mij zelfs bij de Kamer voor. De implicaties worden ook verder uitgezocht. Mijn insteek is om zo veel mogelijk Europees te doen, om te voorkomen dat je of voor consumenten of voor bedrijven het weer ingewikkelder maakt om over de grens zaken te doen c.q. het voor criminelen makkelijker maakt om misbruik te maken van verschillen tussen landen.
Dan vroegen mevrouw Rajkowski en mevrouw Leijten of de werkverdeling tussen het Nationaal Cyber Security Centrum, onder verantwoordelijkheid van collega Grapperhaus, en het Digital Trust Center, onder mijn verantwoordelijkheid, voldoende helder is. Het blijft onze taak om aan in dit geval ondernemers en instellingen duidelijk te maken wie nou wat doet. Maar het past wel onvermijdelijk in de risicofasering, die ik net even oneerbiedig schetste aan de hand van brandrisico's, dat daar waar de risico's groot zijn – die kunnen bij cybersecurity heel groot zijn – ze onder het Nationaal Cyber Security Centrum vallen, ongeacht de vraag of het privaat is. Energiebedrijven zijn privaat, banken zijn privaat, maar de maatschappelijke gevolgen van grote cybersecurityrampen zouden zo groot zijn dat we zeggen: dit is van nationaal belang. VDL, om dat voorbeeld maar even te noemen, is een fantastisch bedrijf, maar als er

iets misgaat is dat een grote ramp voor dat bedrijf maar valt Nederland niet stil. Het is dan ook logisch dat een dergelijk bedrijf via het Digital Trust Center benaderd wordt. Daar heb je dan natuurlijk ook weer het hele palet van groot naar klein. Kleine ondernemers zijn helaas zeer frequent doelwit van cybercriminaliteit; vandaar niet alleen onze voorlichtingscampagnes, maar ook het DTC. De Kamer heeft overigens een belangrijke rol gespeeld bij de totstandkoming daarvan. Het heeft als doel om kennis te verzamelen en te delen met ondernemers, groot en klein.
Kunnen we dat dan voldoende doen? Dat was ook meteen weer de vraag van mevrouw Rajkowski en mevrouw Leijten. Dit is in opbouw, zowel wat betreft het aantal medewerkers als wat betreft de onderliggende regelgeving. Collega Grapperhaus wees er al op dat er twee wetten in wording zijn waarvan ik de afkortingen niet nog een keer zal herhalen, maar die wel benodigd zijn om informatie te kunnen delen. Dat is in Nederland strak gereguleerd. Toen mevrouw Van Weerdenburg wees op de constatering van de Cyber Security Raad over het delen van informatie, ging het ook heel sterk hierover. We hebben in Nederland heel, heel scherp ingekaderd of informatie gedeeld mag worden. Daar is een goede reden voor, maar het gevolg is dus ook wel dat je informatie niet kunt delen zonder wettelijke grondslag. Dat geldt hier dus ook. Terug naar de vraag of het DTC voldoende kan doen. De Kamer is afgelopen zomer geïnformeerd dat de wetgeving in procedure is en dat we op kleine schaal zijn gestart met het delen van informatie. Dat is ook zeer gewenst, maar de achterliggende regelgeving is ook van belang, overigens ook omdat bedrijven zelf weer beschermd willen worden op het moment dat ze informatie delen. Dat begrijp ik ook weer. Je laat ook je eigen kwetsbaarheid zien. Zij willen dan weer voldoende zekerheid hebben dat als ze dat doen, ze vervolgens niet, langs welke route dan ook, aan de schandpaal genageld worden. Zowel vanuit onze eigen privacywetgeving als om ondernemers en bedrijven met een gerust gemoed te laten deelnemen aan informatiedeling hebben we die onderliggende regelgeving nodig. Daarnaast heb je altijd de kwestie van maatvoering, geld en personeel. Dat komt gewoon in de jaarlijkse begrotingsrondes tot u, waarbij de verantwoordelijke Minister altijd zal zeggen: graag meer en uitgebreider. Ik denk dat we die discussie nu niet hoeven te voeren.

De **voorzitter**:
Maar u moet wel even in discussie met de heer Amhaouch, want die heeft een vraag.

De heer **Amhaouch** (CDA):
Dank voor de beantwoording van de Minister. Toch even het voorbeeld van VDL ...

De **voorzitter**:
Liever geen voorbeeld, gewoon een vraag.

De heer **Amhaouch** (CDA):
Anders kan je de vraag niet in de context plaatsen. Het gaat om een bedrijf met duizenden werknemers dat platligt. Met zo veel toeleveranciers is het de vraag hoe we samen – overheid en bedrijfsleven – kunnen komen tot een bepaalde certificering of norm, bijvoorbeeld ISO-normen, in het kader van beveiliging. Hoe stellen we die? Van wie zouden die moeten komen? Dat is eigenlijk de concrete vraag aan de Minister. Als we samen naar een hoger niveau willen om het bedrijfsleven een eigen verantwoordelijkheid te laten nemen om hun dijkverzwaring op orde te hebben, moeten we wel gezamenlijk komen tot gedeelde normen.

Minister **Blok**:

Daar is die maatvoering weer heel cruciaal. Allereerst is er het Europese niveau. Daar gaat de Europese Cybersecurity Act over. Vervolgens moet je op nationaal niveau vaststellen welk type organisatie het is. Soms is het een bedrijf, soms een publieke organisatie. Dat is zo cruciaal dat we ze verplichtingen gaan opleggen, bijvoorbeeld een meldplicht en verplichtingen rondom de periodieke controles rond veiligheid. Wanneer wordt het eigen verantwoordelijkheid? Dat kan in de loop van de tijd verschuiven. Energiebedrijven zijn bijvoorbeeld recent aan de hoogste categorie toegevoegd. Bedrijven die daar niet onder vallen, wat bijvoorbeeld geldt voor dat bedrijf dat ik dan niet meer zal noemen – een mooi bedrijf, van groot belang in de Nederlandse infrastructuur, dat zich overigens zelf ook heel goed bewust is van de kansen en de risico's van ICT – zullen dat dus allereerst zelf doen. Dan kom ik op dat andere instrument uit de gereedschapskist, naast regelgeving. Als er geen bindende regelgeving is voor een dergelijk bedrijf, kom je bij kennisdelen en elkaar informeren. Dat speelt hier dus en dat blijft hier ook spelen. Zij helpen ons en collega's door te vertellen wat er precies gebeurd is. Daarmee kunnen we waarschijnlijk voorkomen dat andere hetzelfde lot treft. Een andere keer kunnen we zoiets voor zijn omdat het nog niet gebeurd is, maar we de dreiging kunnen zien en delen zodat dit bedrijf of een ander bedrijf daar zijn voordeel mee kan doen. Nogmaals, de bereidheid is heel groot van de kant van bedrijven, mits we het wel netjes inkaderen zodat zij zich beschermd voelen en wij die informatie kunnen delen.

De **voorzitter**:
U vervolgt uw betoog.

Minister **Blok**:
Mevrouw Rajkowski vroeg hoe we voorkomen dat er een wildgroei aan keurmerken komt. Ook daarvoor wordt op Europees niveau aan regelgeving gewerkt onder de Cybersecurity Act. Dat is vrijwillige regelgeving. Daar speelt een van de spanningen waarover we het hier wel vaker hebben: hoever gaat de traditionele en belangrijke vrijheid van ondernemers om zelf dingen te doen? Ook het vormen van keurmerken is vanouds iets wat ondernemers en ook niet-commerciële instellingen zelf kunnen doen; denk aan de Echte Bakker. Waarom zou je dat dicht willen reguleren? Tegelijkertijd is er het belang van consumentenbescherming en van helderheid. De Cybersecurity Act gaat uit van vrijwilligheid bij het aansluiten bij richtlijnen en keurmerken, en dan het liefst Europees. Volgens mij is dat op dit moment een verstandige lijn. Het implementatievoorstel ligt bij de Kamer.

De **voorzitter**:
Als het een korte, scherpe vraag kan zijn, mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Het keurmerk wordt nu vrijwillig, maar het zou zo kunnen zijn dat vanaf 2023 de Europese Commissie toch gaat kijken naar verplichte keurmerken. Dan zou het zo fijn zijn als we daar in Nederland al wat eenduidigheid over hebben. Mijn vraag was dus ook gericht op de toekomst.

Minister **Blok**:
Het is nog geen 2023, maar vanuit het oogpunt van consumentenbescherming is een vorm van verplichtendheid, zonder dat je dat generiek gaat doen, wel logisch. Het is dus niet zo dat wij tegen elke vorm van verplichting zijn, maar ik noemde niet voor niets het voorbeeld van de Echte Bakker. Je moet het ook niet onmogelijk maken dat bedrijven zelf met keurmerken werken.

Ten slotte het punt dat mevrouw Van Weerdenburg richting collega Grapperhaus opbracht over sideloaden en de Digital Market Act. Dat gesprek hebben wij, ik dacht vorige week, ook gevoerd. De Digital Market Act is heel erg gericht op het versterken van de positie van consumenten en uitdagers van de grote socialmediabedrijven en wil doorbreken dat je alleen via de App Store – het is onvermijdelijk een overleg met veel Engels en afkortingen – van, ik moet in dit geval toch even het bedrijf noemen, Apple apps kan downloaden. Dat doel steunt de Nederlandse regering, want anders bestendig je de machtspositie van een groot bedrijf en beperk je de consument, die inderdaad heel vaak zo'n iPhone heeft, in zijn keuzevrijheid. Apple heeft de mogelijkheid om aan te geven: als u via mij downloadt, controleer ik ook de kwaliteit. Dat is ook prima. Dan is het hun kwaliteitskeurmerk en kun je daar klagen als je ontevreden bent. Maar Apple heeft dan niet de mogelijkheid om te zeggen: het mag alleen via mijn App Store. Dat is volgens mij ook echt een gewenste situatie, want anders breng je de consument niet in de positie van keuzevrijheid en voorkom je dat nieuwe toetreders ook echt kunnen toetreden. En ja, dat betekent vervolgens dat degene die zo'n app downloadt, zelf verantwoordelijk is voor de kwaliteit ervan. Dat is natuurlijk vaker zo wanneer een consument iets aanschaft.
Het is geen systeemrisico. Dat was de andere vraag aan de heer Grapperhaus: waarom valt dit niet onder de hoge risico's? Het is niet zo dat daarmee een hele vitale infrastructuur kan imploderen. Het kan zijn dat de app niet goed werkt of bijwerkingen heeft. Dat is vervelend, maar het is geen risico voor de vitale infrastructuur.

De **voorzitter**:
Mevrouw Van Weerdenburg, als het echt een korte en scherpe vraag is, want het gaat uit de hand lopen.

Mevrouw **Van Weerdenburg** (PVV):
Ja. Dat het geen risico is, klopt niet. In Canada is het gebeurd dat mensen dachten dat ze de officiële corona-app van de overheid downloadden op hun Androidtoestel, maar dat bleek een nepapp die de toestellen heeft versleuteld. Het kan dus wel degelijk een veiligheidsrisico zijn.

Minister **Blok**:
Ook hier is het weer van belang om onderscheid te maken. Ik ga toch weer even oneerbiedig de vergelijking maken met brandveiligheid: is het een systeemrisico of is het risico dat een huis afbrandt? Dit is heel vervelend, maar het is even vergelijkbaar met het risico dat een huis afbrandt. Dat wil niet zeggen dat je niks moet doen, maar het betekent niet dat je de ultieme maatregel zou moeten nemen dat iemand überhaupt nooit een app mag downloaden die niet door Apple is goedgekeurd. Want dan haal je die hele wet onderuit. Als je toch buiten Apple downloadt, mag dat, maar dan kan het inderdaad zo'n gevolg hebben. Maar ik zou er echt nooit de consequentie aan verbinden dat je eigenlijk de oude monopolieposities die je juist wilde doorbreken, weer terugbrengt. Want dan is het middel echt erger dan de kwaal.

De **voorzitter**:
U vervolgt uw betoog.

Minister **Blok**:
Nou, ik hoop hiermee de aan mij gestelde vragen beantwoord te hebben.

De **voorzitter**:
Kijk aan! Ik kijk even naar de leden. Moeten er nog dingen gevraagd worden? De Minister van Justitie en Veiligheid reageert. Misschien kan hij in een volgend leven voorzitter van deze commissie worden! Mevrouw

Van Ginneken heeft nog een laatste scherpe vraag voor de Minister van Economische Zaken.

Mevrouw **Van Ginneken** (D66):
Dit legt de lat meteen hoog. Ik geloof dat ik iedereen ga teleurstellen. De vraag werd gesteld of alle vragen beantwoord zijn...

De **voorzitter**:
Aan deze Minister.

Mevrouw **Van Ginneken** (D66):
Precies. Ik had verwacht van deze Minister iets te horen op mijn vraag over het activeren van brancheorganisaties om hun rol en verantwoordelijkheid te nemen in cybersecurity. Maar misschien was mijn verwachting onterecht.

Minister **Blok**:
Nee, daar had u inderdaad een antwoord op moeten krijgen. Dat is zeker een route die we graag en ook met regelmaat belopen. Als de achtergrond is dat u het signaal krijgt dat dat onvoldoende gebeurt, dan hoor ik het graag concreter. Dan pakken we dat graag op.

De **voorzitter**:
Nee, mevrouw Van Ginneken, de regering stelt eigenlijk geen vraag terug. Dat is lastig voor de orde van het debat. U bent uitgenodigd om de signalen door te geven, al dan niet in tweede termijn, via schriftelijke vragen of via andere wegen die er zijn voor een Kamerlid. De heer Dassen. Kort en scherp, is dat mogelijk?

De heer **Dassen** (Volt):
Zeker, voorzitter. Ik vroeg me af of de Minister wil reflecteren op het Cyber Security Information Sharing Partnership in het Verenigd Koninkrijk. Is het DTC daarmee in contact en wordt er al over nagedacht of er eventueel mogelijkheden zijn om cyberdreigingen in de toekomst te delen?

Minister **Blok**:
Er wordt samengewerkt, sowieso binnen de EU maar in dit geval ook met het VK. Uw andere vraag is om daarop te reflecteren, maar dit is volgens mij het verstandigste wat we kunnen doen, omdat ook hierbij de dreiging natuurlijk grensoverschrijdend kan zijn.

De heer **Dassen** (Volt):
Voorzitter?

De **voorzitter**:
Ja, als het nodig is.

De heer **Dassen** (Volt):
Ja, heel kort. Het gaat mij voornamelijk om de manier waarop ze het nu in het VK hebben ingericht. Kijken wij er ook op die manier naar? Ze zijn daar nu realtime en sectoraal met verschillende grote en kleine bedrijven bezig om te kijken hoe ze die cyberdreiging zo goed mogelijk kunnen mitigeren. Ik vraag me af of wij daar ook naartoe werken.

Minister **Blok**:
Dan moet ik me er echt even beter over informeren hoe het Engelse systeem eruitziet. Waarschijnlijk weten mijn mensen dat. Dan kom ik daarop terug, ofwel in tweede termijn ofwel schriftelijk.

De **voorzitter**:

Dank. Dan geef ik het woord aan Staatssecretaris Knops van Binnenlandse Zaken. Als u zou willen aangeven hoe u uw betoog een beetje heeft opgebouwd, dan kan ik inschatten wanneer het een goed moment is om interrupties toe te staan.

Staatssecretaris **Knops**:
Dank u wel, voorzitter. Dank voor de gelegenheid om in deze eerste bijeenkomst met deze commissie samen van gedachten te wisselen over een heel belangrijk onderwerp. Ik zou het eigenlijk willen toespitsen op een drietal hoofdthema's: allereerst informatiebeveiliging van de rijksdienst, daarna wat wij binnen de rijksoverheid doen om kennis en ervaringen te delen, en ten slotte hoe wij ook bij de inkoop van systemen rekening houden met de risico's die we lopen.
Voorzitter. Het feit dat wij hier met drie bewindspersonen zitten, geeft aan dat wij de afgelopen jaren eendrachtig hebben samengewerkt op dit thema. Collega Blok zei dat al eerder. We hebben in deze kabinetsperiode voor het eerst in de historie een gezamenlijke digitaliseringsstrategie ontwikkeld met deze drie departementen. Die beperkt zich niet tot deze drie ministeries, maar is uiteindelijk wel een richtsnoer voor de manier waarop alle overheidsorganisaties op rijksniveau zouden moeten gaan opereren. Het is geen statisch document. De wereld waarin wij ons bevinden is buitengewoon dynamisch. Dat betekent dat je, zeker als je spreekt over veiligheid en je beschermen tegen dreigingen van buiten, continu actief moet zijn om bij de tijd te blijven. Het is ook nooit af. Je zult altijd nieuwe technieken moeten kunnen toepassen, en dat in een omgeving waarin de wetgevende kaders dat agile optreden niet altijd juridisch onderbouwen. Dat is al een aantal keer aan de orde gekomen. Je zult in de wetgeving dus continu stappen moeten zetten, en je loopt soms tegen de grenzen van wetgeving aan, allemaal met het doel om uiteindelijk ervoor te zorgen dat die overheidsorganisaties gewoon hun werk kunnen doen in die steeds onveiliger wordende wereld. Dat is dan mijn verantwoordelijkheid.
We hebben eerder al voorbeelden genoemd. Ook een aantal van u heeft die al genoemd. Ransomware is ook overheidsorganisaties niet bespaard gebleven. We hebben in september jongstleden een ransomwareaanval gehad op samenwerkingsbedrijf IJmond. We hebben vorig jaar een ransomwareaanval gehad bij Hof van Twente en bij de gemeente Lochem. Er zijn er nog veel meer te noemen, maar dit zijn wel de grootste. Mijn belangrijkste verantwoordelijkheid zie ik als volgt. Ik ben aan de ene kant verantwoordelijk voor het hele stelsel van de sector Rijk met betrekking tot informatiebeveiliging. Dan gaat het dus om de normenkant: aan wat voor eisen moet je als overheidsorganisatie voldoen om in deze tijd überhaupt veilig te kunnen opereren? Tegelijkertijd ben ik ook verantwoordelijk voor de kant van het openbaar bestuur. Ik moet ervoor zorgen dat de veiligheid bij de organisaties die bij het openbaar bestuur horen op orde is. Dat doe ik in nauwe samenwerking met de collega's van JenV en EZK. Dat laat de ministeriële verantwoordelijkheid onverlet. Die geldt ook nog altijd in ons huis van Thorbecke. Daarbij is elk departement primair zelf verantwoordelijk voor het op orde hebben van de veiligheid, zoals de collega's net aangaven. De analogie met de brand- en inbraakveiligheid is volgens mij een hele treffende. Dat betekent niet dat iedereen dat zelf maar op eigen houtje gaat doen. Nee, die kaderstellende rol is een zaak die BZK in eerste instantie aangaat. In die kaderstellende rol wordt gezegd waaraan wij moeten voldoen en hoe wij daar toezicht op houden.
Voorzitter. Ik kom op de informatiebeveiliging van de rijksdienst. Ik heb de Kamer in een van de brieven uitvoerig geïnformeerd over wat we daar de afgelopen jaren aan gedaan hebben. Ik kan in ieder geval constateren dat het niveau van informatiebeveiliging de afgelopen vier jaar enorm gestegen is. Bijna analoog of spiegelbeeldig aan de omgeving, zou je kunnen zeggen. We hebben daar ook nieuwe rollen en nieuwe sturingsin-

strumenten aan toegevoegd. In de I-strategie Rijk heb ik op basis van de plannen die we gemaakt hebben, aangegeven hoe we de digitale weerbaarheid willen verhogen. We hebben ook de CISO-functie, de Chief Information Security Officer, op alle departementen toegevoegd. Die functie was er daarvoor gewoon niet. Met name aan de veiligheidskant zorgt de CISO er in nauwe samenwerking met JenV en het NCSC voor dat het bewustwordingsniveau van de departementen op een hoger plan komt.
Mevrouw Leijten zei in haar bijdrage dat de Rekenkamer daar ook de vinger op de zere plek heeft gelegd. Dat is ook terecht. Wij hebben op basis van de aanbevelingen van de Rekenkamer ook een aantal maatregelen genomen die ertoe moeten leiden dat het beveiligingsniveau op een hoger plan komt. Mevrouw Leijten zei: als ik de jaarverslagen en de Rekenkamerrapporten van 2019 en 2020 op een rijtje zet, dan zijn er nog steeds vakjes die niet groen gekleurd zijn. Dat klopt. Dat is helemaal waar. Tegelijkertijd kan ik ook zeggen dat er echt wel een aantal stappen gezet zijn. Een voorbeeld is de introductie van de CISO-functie. Maar denk ook aan de halfjaarlijkse voortgangsgesprekken die plaatsvinden tussen CIO Rijk – die zit hier naast me – en CISO Rijk, met alle departementale functionarissen. De aanbevelingen van de Rekenkamer worden daar gewoon heel nadrukkelijk gemonitord. Ook wordt er gekeken hoe die worden opgevolgd.
Ook hier geldt weer: uiteindelijk zijn het in de verantwoordingscyclus de individuele departementen zelf die bij het jaarverslag verantwoording afleggen over het gevoerde beleid en ook hoe dat is uitgevoerd. Een voorbeeld van die monitoring is dat bij BZ, Buitenlandse Zaken, een ernstige onvolkomenheid was geconstateerd. Die onvolkomenheid is niet helemaal weg, maar het is geen ernstige onvolkomenheid meer. Maar dat komt omdat je planmatig, op basis van die analyse, de lekken dicht en de procedures aanpast.
Ik ben zelf ook heel blij met de totstandkoming van deze commissie, waarbij die integraliteit ... Ik zeg het de heer Grapperhaus na. Sorry, ik zeg het de Minister van JenV na. De grote aanwezigheid van verschillende fracties werd in het verleden weleens departementaal en verkokerd neergelegd. Daardoor werden de tegenkracht vanuit de Kamer en de controlerende taak vanuit de Kamer niet helemaal recht gedaan. Dus ik ben zelf heel blij met de bijna organische ontwikkeling hoe we aankijken tegen digitalisering. Het feit dat de Minister van BZK, in casu Staatssecretaris van BZK, naast de Minister van Financiën sinds drie jaar verantwoording aflegt bij Verantwoordingsdag, geeft ook aan hoe de waarde van dit thema zich ontwikkeld heeft. Daar zijn nog heel veel stappen te zetten. Maar ik ben niet ontevreden over wat we daar de afgelopen tijd in gedaan hebben.
Mevrouw Kathmann van de Partij van de Arbeid en de heer Dassen hadden een heel concrete vraag op dit thema. Ik behandel de vragen die gesteld zijn namelijk even per blokje. Ze vroegen zich het volgende af. Wat betekent die hack van SolarWinds nou voor de overheid? Welke rijksdiensten hebben gebruikgemaakt van die software? En welke kwetsbare informatie had eventueel kunnen lekken? De Minister van JenV is daar al in zekere zin op ingegaan. Maar ik zou er nog aan willen toevoegen dat onder coördinatie van CIO Rijk meteen na die hack bij alle organisaties bij de rijksoverheid een uitvraag is gedaan om te achterhalen wie gebruikgemaakt heeft van deze software. Dat is gedaan om een eerste assessment te hebben van de risico's die we lopen. Uiteindelijk bleken vier organisaties binnen de rijksoverheid met deze software te werken. Al die installaties die deel uitmaakten van de inventarisatie bij die organisaties zijn inmiddels gerepareerd. Ook aanvullend onderzoek naar de kwetsbaarheden is uitgevoerd. Er zijn op dit moment en tot nu toe geen sporen van misbruik bekend.

De vraag welke informatie had kunnen lekken door deze hack, is moeilijk te beantwoorden, want het is niet zo dat je, als je eenmaal binnen bent, meteen toegang hebt tot alle informatie. Daar zitten ook nog allerlei firewalls omheen. Het belangrijkste om te constateren is dat deze hack niet geleid heeft tot het kunnen verkrijgen van die informatie, maar dit soort hacks maken ook elke keer weer duidelijk dat die dreiging er is. Die is soms onzichtbaar. Het is anders dan bij brand, maar als je eenmaal mensen binnen hebt en als zij met bepaalde codes toegang tot jouw informatie of zelfs tot jouw systemen hebben, kan dat catastrofale gevolgen hebben. Dat is ook precies de reden waarom het bewustzijn, het erover spreken, dit debat maar het gesprek hierover voeren met overheidsorganisaties en het bedrijfsleven ontzettend belangrijk zijn. Mevrouw Kathmann vroeg ook hoe we als overheid die race tegen dreigingen van buiten op een goede manier aangaan met mensen die geëquipeerd zijn en kennis hebben van deze materie, die zich natuurlijk razendsnel ontwikkelt. De eerlijkheid gebiedt te zeggen dat dat niet gemakkelijk is. De overheid staat op zichzelf nog steeds te boek als een zeer aantrekkelijk werkgever, maar in een arbeidsmarkt waar juist op dit vakgebied aan veel een tekort is, moeten wij noodgedwongen maar wel van harte samenwerken met andere partijen om de kennis die er wel is, te ontsluiten, ook naar de overheid. Dat doen wij bijvoorbeeld door pacten af te sluiten met kennisinstellingen, maar ook door met het bedrijfsleven samen te werken. Op die manier proberen we toch goede mensen aan te trekken, ook omdat de overheid in zekere zin een hele aantrekkelijke werkgever is omdat je de vraagstukken die wij hebben, niet altijd in het bedrijfsleven terugvindt. We hebben daarvoor de RijksAcademie voor Digitalisering opgezet. We werken met I-vakmanschap, met hogescholen en universiteiten, waardoor we mensen die in opleiding zijn, plekken en vraagstukken aanbieden waarmee ze binnen de overheid ervaring kunnen opdoen. Gelukkig kan ik zeggen dat een aantal van die mensen uiteindelijk ook bij de overheid terechtkomt.

De **voorzitter**:
Mevrouw Kathmann, alleen als het een korte vraag is, zonder inleiding.

Mevrouw **Kathmann** (PvdA):
Zo werd de vraag net ook al beantwoord door de Minister, maar mijn vraag is veel groter dan dat. Die gaat erover dat we in het bedrijfsleven, bij de overheid, in de rechtspraak en noem maar op gewoon van mbo tot wo meer mensen nodig hebben die op dit terrein heel breed onderlegd zijn.

De **voorzitter**:
De vraag is helder.

Mevrouw **Kathmann** (PvdA):
Kan in de Cybesecurity Agenda een spoor worden opgenomen dat gaat over die werkgelegenheid en dus over opleiden, herscholen, omscholen, zodat we in de breedte voldoende mensen hebben en zodat dit echt onderdeel wordt van de Cybersecurity Agenda?

De **voorzitter**:
Als de Staatssecretaris dat kan toezeggen, zijn we snel klaar.

Staatssecretaris **Knops**:
Ik kijk met een schuin oog naar de Minister van JenV, want die is natuurlijk de eerstverantwoordelijke. Ja, hij knikt instemmend.

Minister **Grapperhaus**:

Wij zullen er in de tweede termijn wat over zeggen. Met «wij» bedoel ik wij tweeën. Het is geen pluralis majestatis.

De **voorzitter**:
Als er voor twee bewindspersonen nog genoeg tijd is in de tweede termijn.

Staatssecretaris **Knops**:
Het is een terechte vraag van mevrouw Kathmann en het is ook logisch dat dit daar een plek in krijgt. Het heeft overigens onze voortdurende aandacht. Het is niet zo dat er op dit moment echt gaten vallen, maar ik realiseer me zeer dat je, als je twee jaar verder zou kijken, weer praat over hele andere technieken waarmee die aanvallen plaatsvinden. Dit is dus een terecht punt.
Voorzitter. Ik ga naar het tweede blokje: hoe zorg je er binnen de overheid voor dat je die negatieve ervaringen en die aanvallen die zich hebben voorgegaan, omzet in een beter bewustzijn? Ik zie daar een hele belangrijke rol. Die zie ik ook als een soort aanjaagrol, waarin wij niet moeten verslappen. Hoewel al die aanvallen vreselijk zijn, zit er ook een andere kant aan. Elke keer dat er weer zo'n aanval plaatsvindt en een organisatie wordt getroffen, komt er toch een soort wake-upcall bij iedereen: oké, hoe hebben wij dat nu geregeld? Zo hoort het ook. Het is dus niet zo dat wij de verantwoordelijkheid vanuit het Rijk overnemen voor tal van organisaties, maar ik vind wel dat wij het delen van die kennis en die ervaringen moeten faciliteren. Dat doen wij door de overheidsbrede cyberoefening, die sinds 2019 georganiseerd wordt en waaraan tal van partners deelnemen: de Vereniging van Nederlandse Gemeenten, het IPO, de Unie van Waterschappen, maar ook het Nationaal Cyber Security Centrum, samen met EZK en de NCTV. We hebben dezelfde ervaring gehad met covid: we moesten ons een beetje aanpassen. Maar de ervaringen zijn heel positief en de deelname neemt nog steeds toe.
Ik denk dat er geen overheidsorganisatie, geen gemeente en geen provincie meer is waar dit thema niet besproken is. Dat was een aantal jaren geleden anders. Toen was het voor veel gemeenten toch nog een soort ver-van-mijn-bedshow: ze zullen ons niet pakken. Ik denk dat het rijtje dat ik zojuist opnoemde, duidelijk maakt dat elke organisatie getroffen kan worden. De kans daarop is misschien niet eens zo heel groot, maar als je getroffen wordt, kunnen de gevolgen immens zijn. Hof van Twente en Lochem hebben echt gigantische problemen gehad om de overheidsdienstverlening te continueren. Mijn ervaring met de functionarissen die deelnemen aan deze conferentie en oefening, is dat er veel gretigheid is bij overheidsorganisaties om hiervan te leren. We bieden daarbij ook scenario's aan, bijvoorbeeld voor gemeenten, om zelf te trainen en te kijken wat dit voor hun organisatie betekent. We hebben ook een handreiking Red teaming gepubliceerd, waarbij we met ethische hackers overheden uitdagen om daarvan gebruik te maken en te kijken waar de zwakke plekken in hun systemen en organisaties zitten. Dat voelt een beetje ongemakkelijk, want je laat je testen en uitdagen, en daarmee komen de zwakheden bloot te liggen. Maar dit heeft een aantal voordelen. Je weet dan waar de gaten en kieren zitten. Die kun je dichten en de ervaringen die je opdoet, kun je delen met andere overheidsorganisaties. We kunnen gewoon niet onderschatten hoe belangrijk dat is.
Voorzitter. Voordat ik nog inga op een aantal vragen van de leden, ga ik in op de inkoop. Ik denk dat we als overheid een voorbeeldrol hebben in hoe we kunnen inkopen en welke eisen wij stellen aan programmatuur op het punt van ICT-systemen. Je ziet toch dat iedereen anders het wiel opnieuw probeert uit te vinden. Zo kunnen wij helpen om bij onze overheid in ieder geval die systemen binnen te halen waarvan wij weten en verzekerd zijn dat ze veilig zijn. Dat wil niet zeggen dat er daardoor geen zwakheden optreden, want u weet dat systemen een bepaalde veiligheid moeten

hebben, maar dat de menselijke factor, het gebruik daarvan en de procedures net zo belangrijk zijn. Maar ik richt me nu even op de kwaliteit van de systemen. Op basis van de Baseline Informatiebeveiliging Overheid en ook het publiceren daarvan op websites kunnen wij richting andere overheden die faciliterende rol spelen om daarmee ook de veiligheid te verhogen. Dat doen we dus ook steeds meer en meer. Je ziet dat dit bijna stap voor stap organisch steeds beter wordt, dat partijen elkaar steeds beter weten te vinden en dat die kennis dus ontsloten en gedeeld wordt.
Voorzitter, tot slot nog een aantal vragen die door de leden gesteld zijn. Mevrouw Rajkowski vroeg of het kabinet een openbaar onderzoek zou kunnen doen naar de omvang van desinformatie in Nederland en of wij ons er in de EU hard voor kunnen maken om die rapportages te krijgen over desinformatie op sociale media. Op dit moment doet de EU via de Dienst voor Extern Optreden onderzoek naar desinformatie van statelijke actoren. Nederland maakt ook deel uit van het EU Rapid Alert System, waarin informatie over desinformatiecampagnes van statelijke actoren gedeeld wordt. Om begrijpelijke redenen is deze informatie op zich niet openbaar, maar periodiek maakt de EDEO wel openbare rapportages. In het kader van de verbeterde EU-zelfregulering op het gebied van desinformatie moeten socialemediabedrijven wel meer gaan rapporteren over de acties die zij ondernemen tegen desinformatie. Deze rapporten worden dan wel openbaar. Over het precieze moment waarop deze rapporten openbaar worden gemaakt, wordt op EU-niveau nog onderhandeld. Het voornemen is wel om de plannen daarover eind dit jaar te publiceren. De Kamer wordt begin volgend jaar geïnformeerd over het kabinetsstandpunt, dat volgt zodra deze EU-zelfregulering gepubliceerd is.
Ik denk dat ik de vraag van de heer Amhaouch over ransomware heb beantwoord. Hij noemde de voorbeelden van bedrijven, maar vroeg ook wat dit betekent voor overheden. Daar heb ik op gereflecteerd, ook door middel van de Baseline Informatiebeveiliging. 100% garantie kun je natuurlijk niet geven, maar het feit dat het bewustzijn vergroot wordt en dat iedereen acties onderneemt en er ook belang bij heeft om dat te doen, gezien de steeds groter wordende consequenties als je dat niet doet, maakt wel dat we echt veel verder zijn dan een aantal jaren geleden. Die stelling durf ik wel te betrekken. Ik hoop ook dat dit ertoe leidt dat, welke organisatie het ook betreft, ook dit soort vragen telkens gesteld worden, net zozeer als de vraag of er op het eind van het jaar een sluitende begroting is en of de financiën op orde zijn. Ik heb eerder in brieven ook gemeenteraden opgeroepen om dit thema aan de orde te stellen. Het is natuurlijk een technisch thema. Daar zit enige handicap aan. Tegelijkertijd kun je je op dit vlak laten adviseren door experts, maar ik zou willen zeggen dat dit thema niet benoemen een beetje struisvogelpolitiek is. Dit is ontzettend belangrijk voor continuïteit en daarmee ook voor het vertrouwen dat de burgers mogen hebben in de overheid.
Voorzitter, daarmee ben ik volgens mij gekomen aan het eind van de beantwoording van de aan mij gestelde vragen.

De **voorzitter**:
Dan dank ik u hartelijk voor de beantwoording van de vragen. We zitten op 17.00 uur. We hebben nog een uur. Ik zou willen voorstellen dat u maximaal twee minuten heeft in tweede termijn. Het hoeft niet, maar na twee minuten is het wel klaar, ook midden in een zin. Ik heb heel ruim de tijd gegeven voor interrupties. Die waren echt niet allemaal zo kort als waartoe ik af en toe aanspoorde. Ik begin bij mevrouw Rajkowski namens de VVD.

Mevrouw **Rajkowski** (VVD):
Dank u, voorzitter. Ik heb een vraag over het delen van informatie en de AP. Ik begreep dat de wetgeving uiteindelijk naar de Kamer komt. Maar

wanneer komt die dan? Het zou toch zonde zijn als er een digitale ramp plaatsvindt bij een groot niet-vitaal bedrijf en dat we er dan achter komen dat er al een tijdje informatie heeft gelegen bij het NCSC dat het niet mag delen.
Dan over het oefenen en ISIDOOR. De bedrijven schreeuwen er gewoon om om regelmatig te oefenen. Elke twee jaar is toch echt te weinig. Dat wil ik hier even gezegd hebben en onthoud ik voor volgende debatten.
Dank voor de toezegging van Staatssecretaris Knops over de rapportage over desinformatie. Hij informeert de Kamer in januari over het kabinetsstandpunt.
Voorzitter. Ik zou ook nog wat over het delen van kennis willen zeggen. Ziekenhuizen zijn niet als vitaal aangemerkt, terwijl ze op dit moment toch echt een vitale functie in onze maatschappij vervullen. We kunnen geen enkel bed, afdeling of ziekenhuis missen op dit moment. Zou het dus toch mogelijk zijn om ziekenhuizen al dan niet tijdelijk als vitaal aan te wijzen, zodat zij meer toegang krijgen tot het NCSC? Als daar nu geen antwoord op kan komen, dan graag per brief. Dat is ook prima.
Voorzitter. Als laatste wil ik nog over cybercrime zeggen dat misdaad niet mag lonen. Digitaal is dat soms nog te veel het geval. Het ging net over phishing. De VVD is in ieder geval erg blij om te lezen dat de afgelopen week een jongen van 20 jaar die € 40.000 had gephisht, voor drie jaar de bak in is gegaan. Dat geeft een goed signaal af. Dank daarvoor.

De **voorzitter**:
Dank aan u. Dan is het woord aan mevrouw Van Weerdenburg voor haar tweede termijn.

Mevrouw **Van Weerdenburg** (PVV):
Dank, voorzitter. Dank aan de bewindspersonen voor hun antwoorden en voor de geruststellende woorden dat zij goed op de winkel zullen passen totdat het NK, het nieuwe kabinet, er eindelijk is. We konden al lezen dat dat in ieder geval niet voor de kerst zal zijn. Ik twijfel ook niet aan hun inzet op dit punt, maar de realiteit is dat de analyses van de huidige situatie vernietigend zijn. De Cyber Security Raad was helder: de resultaten van de cyberoefening zijn wat rooskleuriger opgeschreven. Maar als je goed leest, is de conclusie dat we niet goed voorbereid zijn op een grote cyberaanval. Dus we kunnen slechts hopen dat internationale cybercriminelen en hackers ons land niet in het vizier hebben de komende weken. Dat is toch enigszins een onrustige gedachte.
Tot slot, voorzitter. Ik ben het helemaal eens met de Minister als hij zegt dat de digitale dijkbewaking op orde moet en dat iedereen zijn steentje daaraan moet bijdragen, ook bedrijven en burgers. Installeer de updates op tijd. Klik niet op «herinner mij later». Denk even wat langer na over een veilig wachtwoord enzovoort, enzovoort. Er ligt voor ons allemaal een taak om daar bewustwording over te verspreiden. Maar laten we het burgers en bedrijven dan niet moeilijker maken dan het nu al is. Daar komt ze weer; door de verplichting om sideloaden toe te staan op bijvoorbeeld iPhones en iPads wordt een nieuw veiligheidsrisico gecreëerd voor bedrijven en burgers. Zoals ik al zei, is dat in Canada gruwelijk misgegaan met de corona-app van de overheid, althans met een app die heel erg leek op de officiële app. Mensen hebben die volledig onbewust geïnstalleerd en die zaten maar mooi met een versleuteld toestel. Minister Blok zegt: dat is geen systeemrisico; het is lullig dat je huis afbrandt maar ... hè? Mijn concrete vraag is: mogen de ambtenaren op zijn ministerie – die vraag wil ik ook aan de Minister van JenV, de heer Grapperhaus, stellen – straks op hun apparaten, iPhones, iPads, ook sideloaden?

De **voorzitter**:

Nogmaals, twee minuten is echt twee minuten. Ik was non-verbaal al signalen aan het geven. Op deze manier moeten we het echt even doen met elkaar. Mevrouw Van Ginneken, u heeft twee minuten. Vijftien seconden van tevoren geef ik een seintje.

Mevrouw **Van Ginneken** (D66):
Voorzitter, ik houd uw non-verbale signalen in de gaten. Als eerste dank voor de antwoorden op mijn vragen over Pegasus en NSO. Ik heb begrepen dat de Minister hier in de openbaarheid niet alles hierover kan zeggen, maar kan hij toezeggen de Kamer daarover vertrouwelijk nader te informeren? Zo kan ik wat specifieker antwoord krijgen op mijn vragen.
Punt twee. Mijn vraag over de Istanbul Conventie is volgens mij niet beantwoord.
Punt drie sluit daar een beetje op aan. Ik heb een wat ongemakkelijk gevoel. Ik ben blij dat u hier met drie bewindspersonen zit, maar dat toont ook de verschotting en versnippering aan, waar ik eerder iets over heb opgemerkt. Mkb-bedrijven zijn niet vitaal, maar leveren wel aan vitale organisaties. Daar zijn discussies over. Horen energieproducenten erbij, horen ziekenhuizen erbij, zo was de vraag van mijn collega Rajkowski. Experts en bedrijven roepen in de internetconsultatie dat de scheiding tussen vitaal en niet-vitaal echt in de weg zit om een goede cyberveiligheid te hebben in ons land. Ik mis hier de overkoepelende visie. Ik zou graag van de verantwoordelijk Minister voor onze cybersecurityagenda echt nog een goede inhoudelijke reflectie horen op het idee om naar één verantwoordelijke uitvoeringsorganisatie te gaan.

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

De heer **Amhaouch** (CDA):
Voorzitter. Ik ga echt mijn best doen om het binnen twee minuten te doen, want ik zou echt niet durven daaroverheen te gaan. Het is belangrijk dat we vandaag in dit eerste commissiedebat over digitalisering hebben gesproken met de drie bewindspersonen. Er is veel voorbijgekomen, maar ik denk dat we ook iets moeten laten aan het NK, dat eraan komt. Anders gaan we vandaag alles oplossen, en dan zijn we te vroeg klaar.
Ik wil drie punten benoemen. Allereerst oefenen, oefenen, oefenen. Het is heel goed dat de oefeningen in het kader van ISIDOOR plaatsvinden, waarbij organisaties worden gestresstest. Wat ons betreft zou dat niet alleen maar een grote oefening hoeven te zijn, zoals mevrouw Rajkowski ook zei. Het kan ook kleinschalig en heel gericht zijn in bepaalde kritische ketens.
Punt twee: ziekenhuizen. In deze fase, waarin we in een coronacrisis en een zorgcrisis zitten, kunnen we niet een theoretische discussie houden over de vraag of ziekenhuizen wel of niet vitaal zijn. Ik ga ervan uit dat de bewindspersoon, en zeker de verantwoordelijk Ministers, daar ook op die manier op acteren. Als morgen alles platligt, zijn we veel verder van huis. Dat is geen theorie, want het is al in meerdere landen gebeurd. Het is ook al gebeurd in Nederland, maar ook in Ierland, Canada en België.
Voorzitter. Het derde punt; daarmee ben ik er al. Ik heb net niet een heel goed antwoord gekregen van de Minister van Economische Zaken op mijn vraag over niet-vitale bedrijven. Dat gaat dus om het gewone bedrijfsleven, het mkb. Hoe komen we daar toch tot een stuk certificering en standaardisatie, zodat we dezelfde taal praten? Dat zou ook goed passen in het MKB-actieplan, waarvan het derde punt certificering is. Het gaat erom dat toeleveranciers, grote bedrijven, kleine bedrijven met elkaar dezelfde taal praten en zichzelf een dijkverzwaring kunnen opleggen.
Ben ik binnen de tijd gebleven, voorzitter?

De **voorzitter**:

Ja. Er wordt hier meegetimed. Hartstikke goed. U heeft goed uw best gedaan, meneer Amhaouch. Bedankt. Dan geef ik het woord aan mevrouw Kathmann.

Mevrouw **Kathmann** (PvdA):
Ik ga deze tijd ook gebruiken om even te zeggen dat mijn vraag over het Clearinghouse niet beantwoord is. Dat is het initiatief van internetgerelateerde organisaties die waarschuwen voor ... O, ik begrijp dat de vraag wel is beantwoord. Dat is misschien gebeurd op het moment dat ik heel even afwezig moest zijn. Sorry.
Dan twee andere dingen. Ik voel terughoudendheid om te verplichten of te verbieden. Toch twee vragen daarover. Als het gaat over misinformatie, komt er bijvoorbeeld in Australië wetgeving om trollenlegers die misinformatie verspreiden en vaak ook op de man spelen, van internet te krijgen. Dat geldt als ze dat anoniem doen. Ik vroeg me af hoe de Minister kijkt naar de wetgeving in Australië en of die misschien ook in Nederland ingesteld zou kunnen worden.
Dan de terughoudendheid over het verplichten van de dijkverzwaring of het instellen van een minimumstandaard daarvoor. Hoe kijkt de Minister aan tegen bijvoorbeeld een cyberaangifte? Je moet laten zien dat je financiële cijfers op orde zijn, maar als je een cyberaangifte doet, laat je in ieder geval een checklist aan het einde van het jaar doen om te kijken of je je dijkverzwaring op orde hebt.

De **voorzitter**:
Mevrouw Rajkowski heeft een interruptie, maar ik wil die eigenlijk niet doen. We hebben volgende week nog een debat. Laten we het dan doen. Ik geef het woord aan de heer Dassen van Volt voor zijn tweede termijn.

De heer **Dassen** (Volt):
Dank, voorzitter. Ik zal het kort houden. Ik wil de Ministers en de Staatssecretaris bedanken. Dank voor de toezeggingen van de Minister van JenV.

De **voorzitter**:
Nu had ik misschien toch die interruptie toe kunnen laten. Maar goed, dat heb ik niet gedaan. Hiermee komen we aan het einde van de tweede termijn van de kant van de Kamer. Kunnen de bewindspersonen direct antwoorden? Ja? Kijk, dat is mooi. Ik geef het woord aan de Minister van Veiligheid en Justitie.

Minister **Grapperhaus**:
Voorzitter. We hebben de spieren nu zo warmgedraaid dat dit moet kunnen. Ik begin met de vraag van mevrouw Rajkowski over de deepfakes. Overigens mijn verontschuldigingen dat ik deze vraag niet meteen kon beantwoorden. Waarom worden deepfakes niet bestempeld als hoog risico in de concept-AI-verordening? Ik weet niet precies wat de exacte overwegingen van de Commissie zijn. Wij denk dat de Commissie systemen als hoog risico heeft bestempeld als daarmee een groot risico is dat er fouten in het systeem sluipen, met nare gevolgen. De conformiteitsbeoordeling die een ontwikkelaar voor hoogrisicosystemen moet doorlopen, zorgt er dan dus voor dat er bijvoorbeeld niet per ongeluk wordt gediscrimineerd. Bij deepfakes gebeurt echter iets heel anders. Mensen kunnen ze gebruiken voor het maken van ongewenst of strafbaar materiaal. Gezien de beperkte fantasie van mensen is dat vaak pornografisch of gebruiken mensen ze om er strafbare gedragingen mee te verrichten, bijvoorbeeld het oplichten van iemand. Deepfakesystemen als hoog risico bestempelen lost denk ik dus ook niet zo veel op, want het gaat vooral om wat de gebruiker ermee doet. Wel moeten we zeker stellen dat het strafrecht en de AVG voldoende toegerust zijn om met deepfakes om te gaan. Juist daarom heb ik dat onderzoek door het WODC laten

verrichten. Dat wordt in januari aan uw Kamer aangeboden. Ik zou dan wel voorstellen dat we snel met de beide commissies, namelijk de commissie Justitie en Veiligheid en deze commissie, misschien zelfs gecombineerd, kijken wat we daarvan vinden en hoe we daarmee verder willen gaan.
Mevrouw Kathmann had de vraag over het meenemen van de strategie in het spoor van werkgelegenheid en opleidingen. De NCSA is onderdeel van de ambitie die gaat over de kennisontwikkeling. Ook hier hebben we, zoals ik in mijn eerste termijn heb aangegeven, een enorme noodzakelijkheid. Er zijn goede private initiatieven. Ook zit het in de fakkel die ik zal overdragen aan een volgend kabinet: maak hier een speerpunt van in de nieuwe integrale cybersecuritystrategie. Daar wordt ook op aangedrongen in het advies van de Cyber Security Raad. Dat advies geeft ook de noodzaak aan van integraliteit, waar OCW weer nauw bij betrokken moet zijn. Ik kan het wel vinden, maar uiteindelijk moet ook vanuit OCW hierop worden ingezet, omdat niet alleen opleidingen van groot belang zijn, maar ook de interesse van mensen om daarnaartoe te gaan.
Voorzitter. Mevrouw Kathmann miste het punt van Clearing House. In het kader van de altijd doorlopende dienstverlening doe ik het gewoon nog een keer. De rol die Clearing House wil uitvoeren, past binnen de ambitie die het kabinet heeft om te komen tot een landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden. Mijn ministerie is ook in gesprek met de initiatiefnemers om te bekijken op welke wijze we dit kunnen opnemen binnen het landelijk dekkend stelsel. Daarbij staat voorop dat het belangrijk is dat het NCSC het overzicht houdt van wat er in Nederland gebeurt en het zo de operationele, coördinerende en crisisrol zo goed mogelijk kan vervullen. We erkennen dat er obstakels zijn op het gebied van informatiedeling. Ik heb dat vandaag al een keer of acht gezegd; mevrouw Kathmann was daar vanochtend ook bij. We moeten zorgen dat we die obstakels met elkaar, uw Kamer en het kabinet, oplossen.
Voorzitter. Dan de vraag over de ziekenhuizen en het wetsvoorstel. Mevrouw Rajkowski vroeg: wanneer komt dat wetsvoorstel? Ik zei, maar ik zal dat nog iets meer expliciteren, dat de AP advies heeft uitgebracht. Dat wordt nu in het voorstel verwerkt. We delen de urgentie over het onderwerp. Ik doe mijn uiterste best om daar een voorspoedige voortgang in te krijgen. Dit betekent dat het de volgende ronde gaat richting de ministerraad en daarna naar de Raad van State.
Voorzitter. Dan de ziekenhuizen: zijn die vitaal of niet? De heer Amhaouch wil ik even zeggen dat de Minister van VWS daar momenteel naar kijkt. De laatste stappen worden gezet. Bij de behandeling van de cybersecuritywet – die werd door uw Kamer omgedoopt tot Wbni omdat dit makkelijker zou zijn voor het publiek – in 2018 heb ik toegegeven dat ik zelf misschien enigszins verrast was dat deze sector er nog niet bij zat. Maar in eerste instantie is dat een keuze van de betreffende sectoren zelf. Maar ik ben het geheel met de heer Amhaouch eens dat we er nu echt heel goed naar moeten kijken. Ik denk dat nu al de ondersteuning plaatsvindt door het NCSC, maar we zouden hopelijk snel moeten horen dat die ook richting vitaal gaat.
Dan toch nog iets over het governancestelsel: moeten we niet toegroeien naar een organisatie met één integrale eindverantwoordelijkheid voor cybersecurity? Als we het te gecentraliseerd doen, krijg je mogelijk een verlies van expertise en verantwoordelijkheid. Vergeeft u mij, voorzitter, dat ik in de schorsing van het debat hardop mijn gedachte uitsprak dat we moeten oppassen dat we straks niet een nationaal coördinator nodig hebben om alle nationaal coördinatoren te coördineren. Ik begrijp die gedachte wel, maar ik heb in de eerste termijn uitgelegd – dat wil ik toch nog eens benadrukken – dat het op dit moment goed is dat we naast het NCSC en de NCTV ook nog steeds de verantwoordelijkheid hebben bij het Digital Trust Center. Degenen die, tussen aanhalingstekens, «onder de een of onder de ander» vallen, hebben een heel verschillend uitgangspunt. Als

je een overheidsinstelling bent, is dat heel wat anders dan als je een private onderneming bent. Maar goed, er is vergaande samenwerking en uitwisseling. Dat is erop gericht om de beschikbare experts zo efficiënt mogelijk in te kunnen zetten en een eenduidig geluid vanuit de overheid te laten horen. In deze decembermaand, waarvan het zeer goed mogelijk is dat dit de laatste maand is dat dit demissionaire kabinet er is, maar misschien ook net niet, vind ik dat we dat echt nog vanuit die indeling moeten doen. Maar ik kan mij voorstellen dat hier in de toekomst zeker nog verder over wordt gedebatteerd met uw Kamer, met name met uw Kamercommissie.
Dan de onlineveiligheid van vrouwen. Daar heb ik in de eerste termijn niets over gezegd. Dat is misschien zo omdat ik daar vanmorgen – mevrouw Kathmann kan getuigen – apart aandacht aan heb besteed. Ik heb dit bij de criminaliteitsbestrijding als apart onderwerp behandeld. Mevrouw Van Ginneken weet dat ik hier echt veel aan heb gedaan en wil blijven doen. Bij mijn aantreden vond ik dat we daar stappen in moesten zetten; ik geef toe dat dit kwam doordat ik geconfronteerd werd met de vrouwen die de MeToobeweging droegen. Die stappen zijn op een aantal punten gezet. Een van die stappen is geweest om ervoor te zorgen dat we volledig volgens het Verdrag van Istanbul werken met toepasselijkheid op alle vormen van geweld tegen vrouwen, met inbegrip van huiselijk geweld, dat vrouwen buitenproportioneel treft. Dat is artikel 2, lid 1. Al dat geweld, zoals stalking, dwingende controle en psychologisch geweld, kan zich ook allemaal online manifesteren. Het verdrag biedt dus al aanknopingspunten om het op dit punt te kunnen bestrijden. Ik zal erop inzetten – dat doe ik op dit moment ook al – om nu juist vanuit het Ministerie van Justitie en Veiligheid te benadrukken dat wat offline geldt, ook online moet gelden. De collega's hebben dat ook herhaald. Al die vormen moeten we dus net zo stevig aanpakken als het om onlinesituaties gaat. Ik kijk even naar de Kamerleden. Ik dacht dat ik hiermee alle vragen heb beantwoord.

De **voorzitter**:
Dan geef ik mevrouw Rajkowski als eerste het woord voor een korte vraag.

Mevrouw **Rajkowski** (VVD):
Dank voor de beantwoording van mijn vraag over het al dan niet tijdelijk aanmerken van ziekenhuizen als vitaal. Ik begreep dat de Minister van VWS daarnaar kijkt. Wanneer krijgen wij als Kamer wat te horen? Dan kan dit wellicht als toezegging genoteerd worden.

Minister **Grapperhaus**:
Nee, daar zou ik niet een toezegging over willen doen. Ik wil veel punten toezeggen, maar ik vind dat ... Kijk, ik heb aangegeven dat ik de urgentie zie van het wetsvoorstel waarin dit ingepast zou moeten worden. We zijn bezig om het advies van de AP daarin te verwerken. Ik kan u verzekeren dat we ondertussen een beleefde aansporing hebben jegens bewindspersonen en departementen waar nog vragen uitstaan, zoals deze. Zo kunnen we in het nieuwe jaar hier snel bij uw Kamer op terugkomen. Ik vind dat ik even geen datum moet noemen uit hoofde van.

De **voorzitter**:
Dan geef ik het woord aan mevrouw Van Weerdenburg voor een korte vraag.

Mevrouw **Van Weerdenburg** (PVV):
Ik had de Minister van JenV gevraagd of zijn ambtenaren straks third-party apps mogen sideloaden op hun Apple-apparaten.

Minister **Grapperhaus**:
Ik heb heel veel verantwoordelijkheden, maar ik ga niet over wat mijn ambtenaren mogen. Daar zal straks de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties op ingaan, want hij gaat over de digitale rijksoverheid en over ambtenaren.

De **voorzitter**:
Mevrouw Van Ginneken heeft ook nog een vraag.

Mevrouw **Van Ginneken** (D66):
Ik slik mijn vraag in. Daar zult u blij om zijn.

De **voorzitter**:
Nou, kijk eens aan! Niemand anders nog? Niet? Dan geef ik het woord aan de Minister van Economische Zaken.

Minister **Blok**:
Dank u wel, voorzitter. De eerste vraag aan mij was ook van mevrouw Van Weerdenburg. Die vraag gaat dezelfde route, omdat omgang met IT niet per ministerie bepaald wordt, maar rijksbreed.
Zowel mevrouw Van Ginneken als de heer Amhaouch ging in op de positie van mkb'ers, die ook vitaal kan zijn in de keten. Zij vroegen hoe we daarbij om kunnen gaan met certificering en standaardisering. Ik grijp dan toch weer terug op de zwaarte van de risico's zoals ik die aan het begin geschetst heb, dus de zwaarte van de risico's voor de samenleving als geheel. Om die in te perken moet je bij een aantal vitale organisaties zware instrumenten inzetten. De term «zwaar» zal ook door de organisatie zo ervaren worden. Iets als een meldplicht, dat is echt wat. De heer Amhaouch heeft zich er vaak expliciet over uitgesproken, maar misschien heeft mevrouw Van Ginneken er soortgelijke opvattingen over, dat we een balans moeten vinden tussen het werkbaar houden van regelgeving voor het mkb en het dienen van veiligheidsbelangen. Het is mogelijk dat een meldplicht die acceptabel kan zijn voor een grote bank of een groot energiebedrijf, niet te dragen is voor een mkb'er. Ook op het moment dat die mkb'er ondanks zijn omvang ergens in een keten een cruciale rol speelt, heeft hij gewoon niet de omvang om zo'n meldplicht te kunnen dragen. Ook daar geldt toch weer een beetje de vergelijking met brand – sorry. Ook bij dat grote bedrijf in Zuid-Nederland dat we niet steeds willen noemen kan brand uitbreken. Dan komt de brandweer en misschien treedt het rampenplan in werking, maar het moest zelf gaan over de blusinstallatie en het voorkomen van brand. Via het Digital Trust Center en onze contacten met bedrijven en branches willen we ze daarbij ondersteunen, maar ik wil echt zorgvuldige maatvoering in wat verplicht is.
De heer Dassen had ik beloofd om nog te kijken of wij iets specifiekere informatie hebben over de Britse evenknie van DTC en NCSC. Die is inderdaad een stap verder als het gaat om de snelheid en het realtime informeren, dus die is een lichtend voorbeeld. Ik gaf al aan dat we contact met hen hebben. We zijn nog niet zover, maar ongeacht het onderwerp vind ik altijd dat Nederland bij de beste vijf in de wereld moet horen, dus dat vind ik hier ook.
Hiermee hoop ik de aan mij gestelde vragen beantwoord te hebben.

De **voorzitter**:
Ik zie dat er geen woordmeldingen zijn, dus dat zal naar tevredenheid zijn geweest. Dan geef ik tot slot het woord aan de Staatssecretaris van Binnenlandse Zaken.

Staatssecretaris **Knops**:
Dank u wel, voorzitter. Allereerst de vraag van mevrouw Van Weerdenburg, die langzaam deze kant op is geschoven. Daarvan zou ik

het volgende willen zeggen. Het was een interessante vraag die ik graag schriftelijk wil beantwoorden. Dat doe ik uiteraard mede namens de collega's van JenV en EZK. Dit vraagt in ieder geval wat nadere doordenking.

De **voorzitter**:
Als dat de inhoud van het antwoord ten goede komt, is dat natuurlijk altijd goed. Wel wil ik opmerken, ook als ordebewaker, dat mevrouw Van Weerdenburg deze vraag inmiddels vijf keer heeft gesteld in dit debat. Ik geef u zo nog de kans om hierop te reageren, maar zou dus de oproep willen doen om deze vraag snel en het liefst zo volledig mogelijk te beantwoorden. U bent volledig vrij om iedere bewindspersoon van wie u denkt dat het goed is in de ondertekening mee te nemen. Maar het is wel een aantal keren gevraagd door mevrouw Van Weerdenburg. Het was een belangrijk punt in haar betoog en in verschillende interrupties.

Staatssecretaris **Knops**:
Zeker, voorzitter, maar ...

De **voorzitter**:
Het is terecht als u zegt dat u het zo beter kunt beantwoorden, maar ik vind het voor mevrouw Van Weerdenburg, die dit een aantal keren te berde heeft gebracht, een ietwat teleurstellende uitkomst. Ik geef haar ook zelf nog het woord.

Mevrouw **Van Weerdenburg** (PVV):
Die conclusie deel ik, maar ik stel u tegelijk gerust. Ik zal hier vaker op terugkomen, maar ik heb geen bezwaar tegen schriftelijke beantwoording. Maar zou de Staatssecretaris dan misschien ook even terug kunnen lezen wat we in het debat over de DMA hebben gezegd? We hebben die discussie ook met Minister Blok gehad. De conclusie was dat eigenlijk niemand over de kwaliteit van de apps van third party appstores gaat. Dat was een redelijk schokkende conclusie, maar dat is dus de realiteit. Kunt u daarop ingaan? Want dit is eigenlijk een black box. Natuurlijk is het ieders eigen verantwoordelijkheid als je dat downloadt, maar ook de goedwillende burger die het niet verkeerd wil doen, kan daarin trappen. Daarom sloeg ik even aan op wat de Minister van EZK zei: «Het is geen systeemrisico». Dat geldt wellicht voor een «privéburger», maar dat is dus anders voor een rijksambtenaar. Vandaar dat ik het toch wel belangrijk vind dat we hier goed op doorvragen.

Staatssecretaris **Knops**:
Zeker. Het feit dat een vraag vijf keer gesteld wordt of dat er geen antwoord op komt, zegt overigens niets over de vraag en over de kwaliteit van de vraag; integendeel. Ik vind alleen dat als ik een antwoord geef, dat antwoord wel doordacht moet zijn. Dit raakt aan veel departementen. Dat is dus de reden waarom ik de vraag graag schriftelijk wil beantwoorden, want de laatste specificatie van de vraag van mevrouw Van Weerdenburg gaat over rijksambtenaren. Dat is inderdaad mijn verantwoordelijkheid, maar er zitten ook een aantal andere aspecten aan, die u ook in het debat heeft genoemd. Het lijkt mij goed dat u, juist recht doend aan uw vraagstelling, een zorgvuldig antwoord krijgt. Vandaar mijn voorstel om dit schriftelijk te doen.
Mevrouw Kathmann vroeg zich af of wat zij «een cyberaangifte» noemde, geen goed idee zou zijn. «Aangifte» associeer ik toch een beetje met een soort belastingaangifte. Als ik het goed heb begrepen, doelde zij op het melding maken door overheidsorganisaties van de staat van de cyberveiligheid.

Mevrouw **Kathmann** (PvdA):

Nee. Bij ondernemers moet de boekhouder zorgen dat de boeken op orde zijn. Je doet dus altijd een soort aangifte of in ieder geval een check of je financiën op orde zijn. Je zou zoiets ook kunnen doen met cyber. Daarmee creëer je in ieder geval bewustwording en heb je een soort minimumstandaard in de zin van: heb je het afgelopen jaar die cyberchecklist afgewerkt?

Staatssecretaris **Knops**:
Dank voor de verheldering. Wij zijn op dit moment met audit- en accountantsorganisaties aan het nadenken en aan het kijken hoe je dit zou kunnen gaan doen. Is daar een model voor te maken dat een soort standaard zou kunnen zijn en daarmee behulpzaam zou kunnen zijn, omdat je daarmee een minimum ... Het kan ook meer zijn dan een minimum. Je toets daarmee een set van eisen, net zoals je dat doet met een accountant die de jaarrekening controleert. Er wordt op dit moment dus al nagedacht over hoe dat vormgegeven kan worden. Dat is één. Twee: bij overheidsorganisaties en departementen valt dit nu al onder de verantwoordelijkheid van de CISO Rijk. In de Jaarrapportage Bedrijfsvoering Rijk rapporteer ik nu al aan de Kamer over dit onderwerp, maar dat ziet dus alleen op de departementen en de rechtstreeks daaronder ressorterende uitvoeringsorganisaties, bijvoorbeeld agentschappen. Daar vallen de zbo's en zo niet onder, maar dit is wel een goed voorbeeld van voortschrijdend inzicht en van ontwikkeling ten aanzien van de eisen die we ook hieraan stellen. Het korte antwoord is dus: daar wordt op dit moment ook over gesproken. Voor decentrale overheden, bijvoorbeeld gemeenten, zou dit ook een model kunnen zijn. Daar reikt mijn verantwoordelijkheid alleen niet toe. Dat is een autonome bevoegdheid van gemeenten.
Dan de vraag of suggestie van mevrouw Kathmann over de wetgeving zoals die in Australië geldt voor desinformatie. Die wetgeving heb ik nog niet helemaal kunnen bestuderen. Ik zou willen voorstellen om deze vraag door te geleiden naar de Minister van BZK, die hier primair verantwoordelijk voor is, zodat hij u informeert over de pro's en cons van een dergelijke wetgeving. Dat zal dan begin volgend jaar worden.

Mevrouw **Rajkowski** (VVD):
Dan zou ik bij dezen toch ook even mee willen geven dat de Australische wet- en regelgeving, waarmee kan worden opgespoord wie allemaal wat online zegt, natuurlijk heel aantrekkelijk klinkt. Dat heeft wel als implicatie dat wij allemaal op te sporen moeten kunnen zijn. Als jij een Twitteraccount, een socialmedia-account of Facebookaccount aanmaakt, moeten zij dus de identiteitscheck kunnen doen, want dat is de enige manier om zeker te weten wie er achter de knoppen zit. Dat vind ik toch wel een hele gevaarlijke route. Bij de afweging die de Staatssecretaris gaat maken, zou ik dus ook de VVD-wens toch even willen meegeven.

De **voorzitter**:
Ik geloof dat het is overgekomen.

Staatssecretaris **Knops**:
Ik weet niet of er nog meer mensen zijn. Zo ja, dan kunnen we ze meteen meenemen naar aanleiding van dit debat. Anders zullen we dat zeker doen. Ik zal het doorgeleiden naar de Minister.

De **voorzitter**:
Dan zijn we aan het eind gekomen van dit debat, maar niet voordat ik de toezeggingen nog eventjes met u heb doorgenomen. Sommige toezeggingen hebben deadlines, andere niet, dus het kan zijn dat ik bij een toezegging even schuin kijk naar een bewindspersoon om te zien of daar

nog een tijdindicatie bij kan komen. Als dat niet het geval is, dan kan dat natuurlijk ook.
– Er komt naar aanleiding van een vraag van de heer Dassen een overzicht van de inzet van middelen voor cybersecurity of digitale veiligheid.
– Er komt een antwoord op de vraag van het lid Leijten over hoe het precies zit met een onderraad, de verslaglegging daarvan en inzicht via de Wob.
– Er is een gegevensveiligheidsmonitor. Dat is een schatting van de maatschappelijke en economische schade. Die wordt nog een keer naar de Kamer gestuurd. Dat was naar aanleiding van een vraag van de heer Dassen.
– Er wordt een overzicht opgesteld van alle campagnes die de afgelopen tijd zijn gevoerd voor bewustwording van online veiligheid en digitale veiligheid. Daarbij wordt ook gekeken naar een vergelijking met andere landen. Door die laatste toevoeging komt die iets later, omdat er iets meer studietijd voor nodig is. Kunnen wij die voor de zomer krijgen?

Minister **Grapperhaus**:
Ja.

De **voorzitter**:
Ja is het antwoord.
– Uiterlijk in «juno ... juno» – hihi – juni 2022 krijgen wij nadere informatie over de implementatie van de aanbeveling over de cybersecurity op Schiphol en de stippenrapportage, naar aanleiding van verschillende vragen van deze Kamer.
– In januari krijgen wij het onderzoek van het WODC over deepfake en over het als hoogrisico meenemen daarvan in de Europese discussie over AI, naar aanleiding van een vraag van mevrouw Rajkowski.
– Er is genoteerd dat de Minister van Economische Zaken nog terugkomt ... Daar ís hij op teruggekomen, dus die toezegging is volgens mij al ingewilligd.
– Dan ben ik bij de Staatssecretaris. De Kamer wordt begin volgend jaar geïnformeerd over het kabinetsstandpunt over de openbaarmaking van EU-rapportages over desinformatie, naar aanleiding van een vraag van mevrouw Rajkowski.
– Op een vraag van mevrouw Van Weerdenburg over het sideloaden krijgen wij schriftelijk antwoord. Daarbij wordt ook ingegaan op de risico's, zeker met betrekking tot de rijksambtenaren.
– Begin volgend jaar wordt de Kamer geïnformeerd over de Australische wetgeving over desinformatie, naar aanleiding van een vraag van mevrouw Kathmann.
Heb ik iets vergeten?

De heer **Dassen** (Volt):
Voorzitter, ik heb een korte vraag. U noemde bij een van de toezeggingen «voor de zomer». Ik zou me kunnen voorstellen dat het wellicht iets eerder mogelijk is om die cijfers te delen. Dat ging specifiek over de bewustwordingscampagnes en de vergelijking met andere landen.

Minister **Grapperhaus**:
In ieder geval voor de zomer van 2022. Help ik daar al mee of is dat nog niet genoeg?

De heer **Dassen** (Volt):
Ik zou verwachten dat dat toch iets ambitieuzer kan.

Minister **Grapperhaus**:

Ik ga mijn uiterste best doen om ervoor te zorgen dat dat er voor 1 april 2022 is.

De **voorzitter**:
Die van «juno» ging over het Algemene Rekenkamerrapport over Schiphol en de cybersecurity daar. Aan de vergelijking van de bewustwordingscampagnes zat nog geen datum, maar er was toegezegd: zo snel mogelijk. Dat werd iets later doordat er een internationale vergelijking wordt gemaakt. Volgens mij zijn we zo rond.
Ik dank u allen voor uw aanwezigheid en voor het debat. Ik zie u allen volgende week heel graag terug voor het eerste beleidsdebat van de commissie voor Digitale Zaken dat dan naar verwachting in de plenaire zaal zal plaatsvinden.

Minister **Grapperhaus**:
Goed, en als u uw schoen zet, krijgt u allemaal nog een boekje.

Sluiting 17.35 uur.