Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 849

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 13 mei 2022

De vaste commissie voor Digitale Zaken heeft op 7 april 2022 overleg gevoerd met mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid, over:

- **de brief van de Minister van Economische Zaken en Klimaat d.d. 30 november 2021 inzake voortgang Roadmap Digitaal Veilige Hard- en Software (Kamerstuk 26 643, nr. 801);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 23 november 2021 inzake voortgang van het implementeren van de ARK-aanbevelingen om de cybersecurity van de grenstoezichtsystemen op Schiphol te verbeteren (Kamerstuk 26 643, nr. 798);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 6 april 2021 inzake onderzoek naar de benodigde investeringen in cybersecurity (Kamerstuk 26 643, nr. 752);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 11 december 2020 inzake reactie op verzoek commissie over het rapport van Amnesty International over massasurveillance (Kamerstukken 26 643 en 32 761, nr. 724);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 14 december 2020 inzake Raadsconclusies over rechtmatige toegang tot versleuteld bewijs (Kamerstuk 26 643, nr. 729);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 14 december 2020 inzake jaarrapportage artikel 18 – Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (Kamerstuk 34 861, nr. 26);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 12 maart 2021 inzake aftapbaarheid OTT-diensten (Kamerstuk 26 643, nr. 748);**
- **de brief van de Minister van Volksgezondheid, Welzijn en Sport d.d. 23 december 2021 inzake reactie op verzoek commissie over het artikel van Computable.nl «VWS werkt aan supertool voor analyse kwetsbaarheden» d.d. 24 november 2021 (Kamerstukken 25 295 en 26 643, nr. 1703);**

kst-26643-849
ISSN 0921 - 7371
's-Gravenhage 2022

- **de brief van de Minister van Justitie en Veiligheid d.d. 17 december 2021 inzake kwetsbaarheid in Apache Log4j (Kamerstuk 26 643, nr. 814);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 16 december 2021 inzake OVV-rapport over kwetsbaarheden in Citrix (Kamerstuk 26 643, nr. 808);**
- **de brief van de Minister van Economische Zaken en Klimaat d.d. 7 februari 2022 inzake voortgang van het Digital Trust Center (DTC) (Kamerstuk 26 643, nr. 817);**
- **de brief van de Minister van Justitie en Veiligheid d.d. 3 maart 2022 inzake Wob-besluiten omtrent Kaspersky (Kamerstukken 30 821 en 26 643, nr. 159).**

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

De voorzitter van de commissie,
Kamminga

De griffier van de commissie,
Boeve

Voorzitter: Van Weerdenburg
Griffier: Van Tilburg

Aanwezig zijn vijf leden der Kamer, te weten: Bontenbal, Van Ginneken, Kathmann, Rajkowski en Van Weerdenburg,

en mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid.

Aanvang 13.32 uur.

De **voorzitter**:
Goedemiddag allemaal. Ik open hierbij deze vergadering van de vaste commissie voor Digitale Zaken. Ik heet u allen welkom. Van de zijde van de Kamer zijn aanwezig de leden Rajkowski van de VVD en Van Ginneken van D66. Mijn naam is Danai van Weerdenburg. Ik zit hier namens de PVV en ik zal als fungerend voorzitter vanmiddag deze vergadering hopelijk in goede banen leiden. Aan de orde is vandaag een debat over online veiligheid en cybersecurity met de coördinerend Minister op dit onderwerp. Dat is de Minister van Justitie en Veiligheid. Ook haar heet ik van harte welkom. Fijn dat u er bent; volgens mij voor de eerste keer. Leuk! We hebben slechts drie uur voor dit debat, dus ik stel voor om snel te beginnen. We zijn niet met heel veel. Ik ga dus niet superstreng op de klok letten. De interrupties wil ik ook niet van tevoren beperken, maar we houden allemaal wel een oog op de klok. De spreektijd is in principe vier minuten. Die hoeven niet per se volgemaakt te worden. Ik denk dat we dan snel gaan beginnen, want er staat genoeg op de agenda.
Mevrouw Rajkowski, mag ik u als eerste het woord geven?

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Misschien nog even een kort puntje van orde om aan te geven waarom we met wat minder mensen zijn. Dat is omdat er nu ook een ander debat loopt. Dit voor mensen die kijken en zich afvragen: goh, waar is de rest van de Kamer eigenlijk?

De **voorzitter**:
Dank u wel, dat was ik nog even vergeten. We hebben een aantal afmeldingen vanwege plenaire debatten die gelijktijdig lopen. Meneer Azarkan en mevrouw Leijten hebben zich afgemeld voor dit debat. Dat heeft er inderdaad niks mee te maken dat het onderwerp niet belangrijk genoeg zou zijn. Het is helaas de gang van zaken, zeker op een drukke Kamerdag.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Elke dag vinden er digitaal miljoenen aanvallen plaats op onze bedrijven, universiteiten en overheid, en dat allemaal in Nederland. Helaas is de schade vaak heel erg groot. Een mkb-ondernemer die gegijzeld wordt met ransomwaresoftware kan klanten en geld verliezen, en soms gaat zelfs het bedrijf failliet. De totale economische schade loopt op tot in de miljarden, geld dat niet geïnvesteerd kan worden in Nederland en in onze toekomst. Het zijn vaak Russische hackers die met een paar drukken op de knop onze bedrijven en instituties, zelfs woning-corporaties, aanvallen, en die daar ongestraft mee wegkomen. Russische cybercriminelen genieten de steun van het Kremlin. Dat is echt niet te verteren. De criminelen hacken alles wat los en vast zit. Dat doen ze ongestoord, zolang ze het maar niet op de Russen zelf richten en zolang ze alle gestolen informatie op commando aan Poetin overdragen.
Voorzitter. Het zijn soldaten in een cyberoorlog, die niet eens de moeite doen om zichzelf te verstoppen. Ze pronken met alles wat ze binnenhalen, want ze denken dat ze toch niet worden gepakt. Het liefst zou ik willen dat we deze gasten van hun bed zouden kunnen lichten en dat we ze voor de

rechter laten verschijnen om zich te verantwoorden. Maar laten we eerlijk zijn, dat is makkelijker gezegd dan gedaan, want het Kremlin houdt dit tuig graag in het spel. Ondertussen lopen deze criminelen lachend binnen. Je ziet ze pochen op YouTube met hun peperdure wagens. Ik zeg: zet ze op de Europese sanctielijsten, zodat ze niet meer bij hun geparkeerde geld kunnen komen en daar in ieder geval niks mee kunnen. Graag een reactie van de Minister.
Voorzitter. Op Europees niveau wordt er hard gewerkt aan een aantal cyberveiligheidseisen die waarschijnlijk pas na 2023 gaan gelden. Cybercriminelen zullen daar niet op wachten. Dat moeten wij dus ook niet doen. Daarom wil de VVD dat de Minister de volgende vier punten meeneemt in haar cybersecurityaanpak om Nederland nu al weerbaarder te maken tegen onlineaanvallen.
Punt één. Het Digital Trust Center is ervoor bedoeld om ondernemers te steunen in hun strijd tegen cybercriminelen, bijvoorbeeld door informatie te delen over aanstaande hacks. Helaas is het DTC vaak nog erg traag met het delen van informatie en worden er ook nog te weinig bedrijven bereikt. Het NCSC heeft vaak soortgelijke informatie over die potentiële hacks die interessant is voor bedrijven, maar misschien ook wel voor gemeenten. Het landschap is te versnipperd. Daarom wil de VVD dat het DTC en het NCSC dichter naar elkaar toe gaan groeien en intensiever en slimmer gaan samenwerken. Graag zien wij dit terug in de nieuwe cybersecurityaanpak.
Twee. Je bent zo sterk als de zwakste schakel. In Nederland kennen we strenge cybereisen voor organisaties die samenwerken met Defensie, waar externe bedrijven aan een soort ABDO-regeling moeten voldoen. Het instellen van strengere eisen zorgt voor een domino-effect en een veilige onlineketen. De VVD wil graag dat de rijksoverheid plannen gaat uitwerken voor een rijks-ABDO. Zo beschermen we samen Nederland.
Drie gaat over het oefenen. Cybersecurity is namelijk topsport. Net zoals in de topsport moet je veel oefenen. ISIDOOR-oefeningen vinden elke twee jaar plaats. Dit zijn grootschalige oefeningen, die daarom ook erg veel voorbereidingstijd kosten. De digitale wereld ziet er twee jaar later wel weer compleet anders uit. Ondertussen is de brandweer juist aan het oefenen op veiligheid, branden en crises op straat. Ik wil eigenlijk die twee werelden met elkaar verbinden, wat op straat gebeurt en de digitale wereld. Die werelden zijn namelijk niet zo gescheiden. Als er online gedoe is, kan je op straat niet pinnen, staan de bruggen open. Daarom wil de VVD een structurele, cross-sectorale oefenagenda voor cyberaanvallen, waarbij zowel grote alsook kleinschalige oefeningen meerdere keren per jaar worden uitgevoerd.
Voorzitter. Dan het vierde en laatste punt: één keurmerk voor onze parels, de mainports. De Cyber Security Raad Nederland noemt de versnipperde cybersecurityaanpak als een van de belangrijkste verbeterpunten om Nederland digitaal weerbaarder en veiliger te maken. Zo zijn er allerlei mooie cybersecuritykeurmerken te vinden, maar het zijn er wel heel erg veel. Daarom wil de VVD dat er bij onze belangrijkste plekken in Nederland, zoals bij Brainport Eindhoven en de Rotterdamse Haven, wordt ingezet op één algemeen keurmerk dat wordt omarmd door DTC en de mainports. Dit schept ook duidelijkheid voor de mkb'ers die daar zaken doen. Een voorbeeld is het keurmerk CYRA. Ziet de Minister hier mogelijkheden voor?

De **voorzitter**:
Dank u wel, mevrouw Rajkowski. Nog net binnen de tijd. Ondertussen zijn ook aangeschoven: mevrouw Kathmann van de PvdA en de heer Bontenbal van het CDA. Ik geef nu het woord aan mevrouw Van Ginneken van D66.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter. Het conflict in Oekraïne: ik kan er niet omheen. De Amerikaanse president, Biden, waarschuwde dat Rusland van plan is om wraak te nemen op iedereen die Oekraïne digitaal steunt. Deelt de Minister deze observatie? Wat betekent dat concreet voor de cyberrisico's die Nederland nu loopt? Wat gaat de Minister op korte termijn doen om die risico's te beperken?
We moeten onze maatschappij sowieso weerbaarder maken tegen cyberaanvallen. Collega Rajkowski noemde dat al uitgebreid. We zien de laatste jaren een toename in ransomware en hacks. Bedrijven moeten zich schrap zetten voor een verdere toename. Hoe zorgt de Minister ervoor dat het bedrijfsleven deze urgentie ook ziet en op de korte termijn ook gaat handelen? Hoe gaat de Wet bevordering digitale weerbaarheid bedrijven daarbij helpen? Waarom is deze wet eigenlijk vertraagd?
Voorzitter. Deze weerbaarheid kan alleen worden gewaarborgd als er voldoende capaciteit is. De basis moet op orde zijn. De Minister moet daarbovenop zitten. Wat vindt de Minister van de conclusie van de Cyber Security Raad dat er meer dan 800 miljoen euro bij moet om onze cyberveiligheid te waarborgen? Hoeveel geld gaat de Minister precies besteden aan de verschillende specifieke onderdelen van cyberveiligheid? Het coalitieakkoord geeft daarover geen uitsluitsel.
Het Nationaal Cyber Security Centrum, het NCSC, speelt hierin een belangrijke uitvoerende rol. Wat D66 betreft moet deze rol groter worden. Het NCSC moet meer mogelijkheden krijgen om naast onze vitale infrastructuur ook andere organisaties en bedrijven te beschermen, zodat het zijn naam, «Nationaal» Cyber Security Centrum, ook echt gaat waarmaken. Want aanvallen op scholen, woningcorporaties of onze voedselvoorziening zorgen ook voor maatschappelijke onrust en ontwrichting. D66 is daarom blij met de nieuwe Europese richtlijn NIB2, die hierin gaat voorzien. Alleen, die richtlijn zal pas na 2024 komen. We kunnen hier al op voorsorteren, want de richting is duidelijk: meer centrale uitvoering over meer sectoren heen.
Het NCSC gaf eergisteren tijdens de briefing ook aan dat expertise schaars is en dat we deze kennis niet te veel moeten verspreiden. Ook het recente OVV-rapport pleit voor concentratie van taken. D66 ziet ook graag dat de slimste cybersecuritymensen van Nederland nu al onder één dak gaan samenwerken. We moeten versnippering terugdringen, in plaats van vergroten, zoals nu gebeurt met de oprichting van het nationaal coördinatiecentrum, NCC, onder de Minister van Economische Zaken. Waarom is dit NCC niet ondergebracht, zo vraag ik de Minister, bij het NCSC of DTC? Kan de Minister toezeggen om al voor de inwerkingtreding van NIB2 toe te werken naar meer concentratie van taken bij het NCSC? Wanneer gaan we afscheid nemen van de scheiding tussen NCC, DTC en NCSC? Excuus voor al die afkortingen. Welke concrete stappen gaat de Minister nemen om daar te komen?
Met de komst van de nieuwe Wbni gaat het NCSC al meer informatie met meer organisaties delen. Maar dat betekent ook meer toezichtwerk voor de Autoriteit Persoonsgegevens. Kan de Minister aangeven hoeveel extra werk er bij de AP ontstaat en of er eigenlijk wel voldoende capaciteit voor is?
Voorzitter. Encryptie is een essentieel onderdeel van onze veiligheid en de bescherming van onze kenniseconomie en democratie. D66 bewaakt dit al jaren. U begrijpt dus wel dat mijn fractie schrok toen we hoorden dat de Minister onderzoek wil doen naar technische oplossingen voor toegang tot versleutelde communicatie. Wie een achterdeur bouwt, kan niet garanderen dat die alleen door bevoegde binnendringers wordt gebruikt. Daarom heeft D66 samen met de VVD schriftelijke vragen gesteld, waar we graag nog de antwoorden op ontvangen.
Ik heb nog twee aanvullende vragen. Wat betekent de grondwetswijziging van afgelopen woensdag over de onaantastbaarheid van digitale

informatie in de cloud voor het beleid van de Minister op dit punt? Kan de Minister toezeggen dat zij de Europese Commissie zal aansporen om in de Europese inventarisatie van toegangsmogelijkheden tot versleuteld bewijs het recht op onaantastbaarheid van digitale communicatie mee te nemen? Tot slot, voorzitter. In de jaarlijkse State of the Union sprak Von der Leyen over de belangrijke ambitie om onze krachten in Europa te bundelen op het gebied van cyberveiligheid. Hoe kan volgens de Minister Nederland als cybergrootmacht hier een leidende rol in spelen? Ik kijk uit naar de beantwoording.

De **voorzitter**:
Dank u wel, mevrouw Van Ginneken. Dan geef ik nu het woord aan mevrouw Kathmann.

Mevrouw **Kathmann** (PvdA):
Dank, voorzitter. Ik wil op voorhand wel zeggen dat ik dit toch een ingewikkeld debat vind. Ik denk dat we in de commissie Digitale Zaken moeten uitmaken hoe we daar in het vervolg mee omgaan. Als je kijkt naar de dingen die op de agenda staan, dan mis je gewoon wel de blik van de Minister van Economische Zaken. Ik denk dat dat vooraf misschien al is gezegd, maar ik kwam door een ander debat helaas later binnen. Je mist structureel eigenlijk gelijk de Staatssecretaris voor Digitalisering. Ik ben overigens wel blij dat deze Minister er is, maar ik vind dat dat echt het debat tekortdoet en dat we daar een oplossing voor moeten vinden. Ik hoop ook dat het kabinet of misschien deze Minister ook op een oplossing wil reflecteren, als dat zou kunnen. Dus dat is mijn eerste vraag.
Dan de onlineveiligheid en cybersecurity.

De **voorzitter**:
Ik ga u even onderbreken, want u heeft een vraag van mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Dank aan collega Kathmann, want dat is op zich een begrijpelijke vraag die gesteld wordt. Maar mijn vraag aan collega Kathmann is dan: stelt de PvdA dan voor om de centrale eindverantwoordelijkheid voor cybersecurity, die nu bij de Minister van JenV ligt, daar weg te nemen en elders te beleggen in het kabinet?

Mevrouw **Kathmann** (PvdA):
Idealiter wel. Het is ook weer lastig om die bij de Staatssecretaris voor Digitalisering te beleggen, maar daar zou wel mijn voorkeur naar uitgaan. De Partij van de Arbeid voelt zich er het meest senang bij als die integrale blik, die heel hard nodig is, geborgd wordt. Het klinkt zo logisch om de Minister van JenV te zetten op cybersecurity, maar dat is het niet. Cybersecurity vraagt ook om andere blikken op veiligheid. Dus ja.

De **voorzitter**:
Mevrouw Rajkowski heeft ook nog een vraag.

Mevrouw **Rajkowski** (VVD):
Ik begrijp de oproep en de wens van mevrouw Kathmann om een breed debat met elkaar te voeren over cybersecurity. We hebben deze keer tijdens de procedurevergadering met z'n allen besloten om de coördinerende bewindspersoon op cybersecurity hier uit te nodigen. We zouden natuurlijk altijd een debat kunnen doen waar meerdere bewindspersonen bij zitten. Dat moeten we van tevoren zelf regelen. Volgens mij zat het 'm niet in onwil of onhandigheid, maar hebben we er als commissie specifiek een uitspraak over gedaan.

De **voorzitter**:
Ja. Daar wil ik even op aanvullen dat we als commissie de Staatssecretaris voor Digitalisering vrijaf hebben gegeven voor dit debat, omdat wij volgende week met haar spreken over informatiehuishouding. Mevrouw Kathmann mag nog even reageren op mevrouw Rajkowski en vervolgt dan haar betoog.

Mevrouw **Kathmann** (PvdA):
Daar hoef ik eigenlijk niet op te reageren, want mijn inleiding was niet bedoeld om een kat te geven aan het kabinet of de Minister die er wel zit. Ik wil u vooral bedanken. Het is meer dat ikzelf als Kamerlid gewoon een worsteling voel. Als je in je voorbereiding zit, merk je dat dit vraagt om een integrale blik. Dat zit ook wel in mijn bijdrage. Ik vind het gewoon heel lastig. Ik denk dat sommige onderwerpen hierdoor niet goed besproken worden. Dat is jammer.
Dan wil ik graag naar de Roadmap Digitaal Veilige Hard- en Software. Dank voor die derde voortgangsrapportage. Ik zie ook dat er wel een hoop dingen gedaan worden, maar ik mis de concrete doelen. Het doel van de PvdA is bijvoorbeeld duidelijk. Wij willen dat vooral de digitale veiligheid van de publieke zaak op één staat. Dan heb ik het over onderwijs, ziekenhuizen, politie, woningbouwcorporaties – vandaag natuurlijk weer in het nieuws – zorg- en welzijnsorganisaties en gemeenten. Ik zou dan ook graag zien dat het kabinet daar de regie op pakt en dat het publieke belang geborgd wordt, ook door bijvoorbeeld veel meer regie te pakken in de ontwikkeling en het gebruik van hardware, en hier dan met name software, bijvoorbeeld in het onderwijs. Noem het digitale-industriepolitiek. Dat helpt niet alleen om het publieke belang te beschermen, maar dat helpt ook onze eigen digitale ondernemers en dus ook die vuist tegen big tech. Dus ik hoor graag van de Minister wat de concrete doelen van dit kabinet zijn aangaande de Roadmap Digitaal Veilige Hard- en Software. Hoe wordt die roadmap op dit moment geëvalueerd? Zonder concrete doelen lijkt me dat heel erg lastig. Hoe wordt de Kamer daarover geïnformeerd?
Dan het rapport van Amnesty International over massasurveillance. Ik vind het niveau waarop er vanuit het kabinet gecommuniceerd wordt over dit onderwerp eigenlijk ook stuitend. Je krijgt een beetje het gevoel dat Amnesty hier wordt weggezet als een of ander onbenullig clubje. Dat is natuurlijk niet zo. Het is gewoon een gerenommeerde internationale mensenrechtenorganisatie. Je hoeft het niet altijd met hen eens te zijn. Ja, ze hebben af en toe hun lobby ook goed op orde. Maar nu worden er echt verantwoordelijkheden weggeschoven op het gebied van mensenrechten, omdat het kabinet voor mijn gevoel bang is dat hun anders iets verweten wordt of dat ze verantwoordelijk worden gehouden voor iets.
Voorzitter. Deze Minister en ik hebben al eerder gesproken over die schijntegenstelling tussen veiligheid en privacy. Toen zei de Minister ook: daar moeten we eigenlijk vanaf. Want door die valse tegenstelling in de lucht te houden, doen we Nederland veel tekort, zeker bijvoorbeeld als we het hebben over die proeftuin in Roermond. Het is niet zo dat wie tegen die proeftuin is, tegen veiligheid is en dat wie voor de proeftuin is, lak heeft aan privacy. Maar hier worden wel op een grove manier mensenrechten geschonden als het gaat over privacy, wat door dit kabinet wordt weggezet alsof er niks aan de hand is. Dus mijn concrete vraag aan de Minister is: kan de Minister toezeggen dat met die proeftuinen wordt gestopt zolang de juiste waarborgen er niet zijn? Dat is namelijk waar het over gaat. Je zou die proeftuinen kunnen doen als je maar zorgt voor voldoende toezicht vooraf en achteraf, als je maar zorgt voor die mensenrechtentoets. Ik zou ook graag van de Minister een reflectie willen hoe zij naar dit vraagstuk kijkt, naar die schijntegenstelling, en hoe die waarborgen in het vervolg wel geborgd gaan worden.

Dan kort over het Kaspersky Lab. Onderaan de brief wordt duidelijk gezegd dat de voorzorgsmaatregelen eigenlijk alleen gaan over antivirussoftware. Mijn vraag daarbij is waarom dat eigenlijk, gezien de actualiteit, niet ook gaat over de andere producten en diensten.
Tot slot cybersecurity, de budgetten en de integrale blik. Ik wilde het al zeggen, maar mijn collega van D66 was me voor. Ik sluit me bij haar aan. Dat geldt ook voor de vragen over de Autoriteit Persoonsgegevens.

De **voorzitter**:
Dank u wel. Dan geef ik nu het woord aan de heer Bontenbal.

De heer **Bontenbal** (CDA):
Dank, voorzitter. Beruchte criminelen, onder wie Ridouan Taghi, gebruikten extra goed beveiligde telefoons om met elkaar te kunnen communiceren. Deze beveiliging wordt wel PGP genoemd, Pretty Good Privacy. Bij de vervolging van deze criminelen is een server in Canada in beslag genomen waarvan deze PGP-telefoons gebruikmaakten. Dat heeft bewijs opgeleverd dat is gebruikt voor de vervolging van zware criminaliteit.
Voorzitter. Versleuteling van berichten, encryptie, belemmert de opsporing van maatschappij-ontwrichtende criminaliteit, zoals cocaïnehandel, kinderporno, enzovoorts. In deze Kamer is ook eerder discussie gevoerd over de vraag of encryptie niet verboden moet worden. In de brief aan de Kamer schrijft het kabinet: rechtmatige toegang tot digitale gegevens is steeds belangrijker voor bevoegde autoriteiten om strafbare feiten op te sporen en de nationale veiligheid te beschermen. Dit geldt bijvoorbeeld voor de aanpak van zware en ernstige criminaliteit en terrorisme. Gezocht is naar technische oplossingen om enerzijds de beschermende waarde van versleuteling hoog te houden, terwijl de negatieve effecten voor opsporings-, inlichtingen- en veiligheidsdiensten worden verminderd.
Voorzitter. Het gaat hier om de botsing van fundamentele waarden, zoals het recht op eerbiediging van de persoonlijke levenssfeer, het communicatiegeheim en de uitoefening van de vrijheid van meningsuiting. Maar zoals het kabinet ook schreef, het recht op privacy is echter niet absoluut. Artikel 8 van het EVRM bepaalt dat een staat dit recht mag beperken als dat bij de wet is voorzien en in de democratische samenleving noodzakelijk is op grond van een aantal nader aangegeven gronden, waaronder de nationale veiligheid en het voorkomen van strafbare feiten. Mijn vraag aan de Minister is hoe zij deze belangenafweging nu maakt als Minister in dit kabinet. Het gevoelen van mijn fractie is dat de balans te vaak doorslaat naar de kant van de privacy en de vrijheid van meningsuiting, maar dat er te weinig oog is voor de maatschappelijke ontwrichting als gevolg van zware criminaliteit. Ik hoor graag uw reflecties daarop.

Mevrouw **Van Ginneken** (D66):
Ik hoor de heer Bontenbal een pleidooi houden voor het inbouwen van achterdeurtjes in encryptie, zoals ik dat ook zojuist in mijn inbreng noemde. Wat ik daar jammer aan vind is dat ik in het betoog van de heer Bontenbal niks hoor over alternatieven die er zijn, zoals de bevoegdheid tot opname van vertrouwelijke communicatie of het op afstand binnendringen in een geautomatiseerd werk. Die laatste bevoegdheid wordt op dit moment ook geëvalueerd, dus ik heb een beetje het idee dat de heer Bontenbal voor de muziek uit loopt. Laten we eerst eens even kijken hoe effectief alternatieven zijn die opsporings- en inlichtingendiensten al hebben om juist die ontwrichting die de heer Bontenbal terecht schetst aan te pakken voordat we encryptie het raam uit gaan gooien.

De heer **Bontenbal** (CDA):
Was dit een vraag of was dit een betoog?

Mevrouw **Van Ginneken** (D66):
Mijn vraag is: waarom heeft de heer Bontenbal dit bredere perspectief van andere bevoegdheden niet opgenomen in zijn pleidooi?

De heer **Bontenbal** (CDA):
Het simpele antwoord is dat ik slechts vier minuten spreektijd heb. En ik heb in mijn betoog niet gezegd dat we die achterdeurtjes moeten maken. Ik heb beschreven wat er in de brief staat. Ik heb een aantal quotes gegeven. En ik heb vooral het dilemma geschetst tussen enerzijds maatschappij-ontwrichtende criminaliteit die mogelijk wordt door encryptie en de andere waarden, zoals privacy en vrijheid van meningsuiting. Ik ben gewoon benieuwd hoe deze Minister in dit kabinet daarnaar kijkt. Ik vind dit een heel belangrijk punt. Ik denk dat we weleens zijn doorgeschoten naar met name het belang van de ene kant en te weinig het belang van de andere kant hebben benadrukt. Maar over welke technologie we specifiek moeten gebruiken heb ik helemaal geen mening.

Mevrouw **Rajkowski** (VVD):
Dan wil de VVD graag ook nog even een duit in het zakje doen, want de hele encryptiediscussie begrijp ik. Die speelt niet alleen hier maar ook in de samenleving. Als we even een paar stappen vooruitdenken – want dat is ook onze rol als politiek: over de toekomst nadenken – dan maak ik me niet zo veel zorgen over encryptie, maar veel meer over kwantumtechnologie. Dus zouden we niet juist moeten gaan nadenken over wat voor impact toekomstige technologieën gaan hebben op hoe wij veilig met elkaar kunnen communiceren? Veiligheid is je eigen veiligheid van de berichten, maar ook hoe de diensten onze veiligheid kunnen waarborgen. Kunnen we in die vlucht naar voren het CDA een beetje aan onze zijde krijgen als we ook wat verder kijken naar ontwikkelingen waar bijvoorbeeld China mee bezig is?

De heer **Bontenbal** (CDA):
Daar wil ik zeker met u over nadenken, heel interessant.

De **voorzitter**:
U vervolgt uw betoog en u heeft nog twee minuten.

De heer **Bontenbal** (CDA):
Mijn tweede punt gaat over die Europese richtlijn voor radioapparatuur. In het najaar heeft de Europese Commissie bekendgemaakt dat wettelijke digitale veiligheidseisen gesteld zullen worden aan draadloos communicerende apparaten in het kader van die richtlijn die ik zojuist noemde. Er zijn de afgelopen jaren verschillende onderzoeken gedaan waaruit blijkt dat we vaak te makkelijk omgaan met de veiligheid van smart home- of smart energy-apparaten. De nieuwe veiligheidseisen gaan gelden voor nieuwe apparaten, maar hoe zorgen we er ook voor dat consumenten zich bewust worden van de risico's van deze apparaten?
Uit het rapport over de integrale aanpak cyberweerbaarheid blijkt dat de cyberveiligheid van vitale processen en infrastructuur een belangrijk aandachtspunt blijft. Hoe beoordeelt de Minister de stand van zaken op dit moment? Zijn we als land genoeg weerbaar als er een verstoring optreedt in vitale processen, zoals de stroomvoorziening, de telecommunicatie en het betalingsverkeer? Zijn vitale processen voldoende opgewassen tegen spionage en sabotage door bijvoorbeeld statelijke actoren?
Tot slot zou ik ons verkiezingsprogramma willen citeren, want de digitale revolutie brengt ons veel goeds, maar er is ook een donkere keerzijde. Dan quoot ik: «De nieuwe technologie vraagt om een nieuwe moraal en de borging van grondrechten van burgers. Fake news, cybercrime, digital profiling, spionage en ongewenste beïnvloeding vragen om een actieve bescherming en reguliering.» Daarnaast moeten we waarden als privacy,

rechtvaardigheid, menselijke waardigheid en een grondrecht als huisrecht actief beschermen. Alleen als de menselijke waardigheid onze toetssteen blijft, kunnen we ook in de digitale samenleving echt een samenleving blijven.
Dank u wel.

De **voorzitter**:
U ook bedankt. Dan ga ik nu mevrouw Van Ginneken vragen of zij even tijdelijk het voorzitterschap wil overnemen van mij, zodat ik mijn inbreng kan doen namens de PVV.

Voorzitter: Van Ginneken

De **voorzitter**:
Dat wil ik. Dan geef ik bij dezen het woord aan mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Zoals ik al vreesde, heeft de collega van D66 al een heleboel dingen genoemd, dus ik ga eventjes een verkorte versie maken. Want de PVV had ook wel vragen bij de organisatiestructuur, met in gedachten de dringende oproep van de Cyber Security Raad om tot een integrale aanpak te komen. Wij maken ons toch wel zorgen om het aantal organisaties dat nu bezig is met cybersecurity en cyberweerbaarheid. We vragen ons af of dat inderdaad niet gestroomlijnder kan. Natuurlijk is er geen enkel bezwaar tegen goede samenwerking, en dat horen we ook elke keer weer terug van alle organisaties: nee, het gaat helemaal prima, we weten elkaar te vinden. Daar is niks op tegen, maar als er een crisis is, een cyberaanval of wat dan ook, dan is er dus geen tijd te verliezen. Snelle informatieverspreiding kan op dat moment veel ellende voorkomen. Dat heeft dan toch de voorkeur.
Dus als die informatie dan langs tientallen schakelpunten moet, lijkt me dat nadelig, want dan verlies je tijd. Dat deed mij een beetje denken aan de sneeuwbal die wij vroeger hadden op school, zo'n soort belschema, mocht het eerste lesuur uitvallen, dat iedereen elkaar moest bellen. Als je dan de pech had om helemaal onderaan het alfabet te staan – misschien herkent de Minister dit zelfs wel – dan werd je soms gebeld als je al vertrokken was richting school. Dat was natuurlijk in het stenen tijdperk, vóór de mobiele telefonie, dus daar had je dan toch wel de balen van. Dan had je dus pech. Hoe gaan wij voorkomen dat organisaties aan het einde van de lijn, aan het einde van die sneeuwbal, straks door pech te laat bereikt worden, met alle gevolgen voor hun onderneming van dien?
Wij hebben afgelopen dinsdag een technische briefing gehad met het NCSC en vertegenwoordigers van de NCTV over de Wbni, waar het NCSC terecht om zit te springen. Want ze krijgen een hele lading kritiek over zich heen, ook van de OVV in het rapport over Citrix, dat ze bepaalde informatie niet gedeeld hebben. Dat straalt slecht op hen af, terwijl ze daar in feite niets aan kunnen doen: ze hebben die informatie, maar mogen die op dit moment niet delen, terwijl ze dat wel heel graag willen. Ik hoor graag van de Minister hoe zij dit zo snel mogelijk gaat oplossen en of er ook een mogelijkheid is om tijdelijk iets te doen, totdat die Wbni er is.
Ik wil haar vragen om daarbij ook niet te schuwen om eventueel heilige huisjes om te schoppen, als dat nodig is. Wij willen daarover als commissie graag meedenken. Als het niet werkt, dan moeten we het anders inrichten. Wat dat betreft zijn prestigeoverwegingen dan niet op hun plaats.
Is de Minister bereid om te laten onderzoeken op welke manier het NCSC en het DTC wellicht geïntegreerd zouden kunnen worden? Mevrouw Van Ginneken had het daar ook al over. Ik heb goed geluisterd naar de directeur van het NCSC afgelopen dinsdag. Hij zei inderdaad dingen als:

versnippering is niet goed, de samenwerking met DTC moet beter, goede expertise over cybersecurity is schaars, je zou die dingen het liefst fysiek onder één dank willen krijgen. Hun eigen organisatie, het NCSC, werkt op de top van hun kunnen, maar de spoeling wordt wel dun. Ze zijn maar met 170 personen en hij had het over een toch beperkte wendbaarheid. Op een gegeven moment zit je aan je max. Ik zal het hem niet letterlijk in de mond leggen, maar ik interpreteerde zijn woorden toch zo dat hij eigenlijk vroeg: kunnen we niet kijken of we wat kunnen samenvoegen om slagkracht en efficiëntie te verbeteren?
Tot slot nog één puntje, want ik ben ook al bijna aan mijn tijd. De kwetsbaarhedenanalysetool die ontwikkeld is bij VWS. Ik vond dat een interessante brief en ik vroeg mij af of meer ministeries dat in gebruik gaan nemen. Goed voorbeeld doet goed volgen. Zijn daar plannen voor? Is dat al gebeurd? Hebben andere ministeries ook zo'n veiligheidsscan, een CAT-scan, aangeboden gekregen vanuit VWS en wat kan de Minister ons daar nog meer over vertellen?

De **voorzitter**:
Dank, mevrouw Van Weerdenburg. Dank ook voor uw ontboezeming over de ervaringen met de belboom op de middelbare school. Ik denk dat dat voor veel mensen herkenbaar is. Ik geef u graag het voorzitterschap terug.

Voorzitter: Van Weerdenburg

De **voorzitter**:
Dank u wel. Ik kijk even naar de Minister. Hoeveel minuten heeft zij nodig?

Minister **Yeşilgöz-Zegerius**:
Ik heb in ieder geval 25 minuten nodig, en dat is ook omdat de ambtenaren heel ver weg zitten. Een deel rent nu deze kant op om tijd te winnen, maar ze zitten echt heel ver weg.

De **voorzitter**:
Oké, dan gaan wij dat doen.

De vergadering wordt van 14.00 uur tot 14.25 uur geschorst.

De **voorzitter**:
Goedemiddag. We gaan verder met deze vergadering van de vaste commissie voor Digitale Zaken. Ik geef het woord aan de Minister van Justitie en Veiligheid voor haar beantwoording.

Minister **Yeşilgöz-Zegerius**:
Veel dank, voorzitter. Hartstikke mooi om met deze Kamerleden dit debat te mogen voeren, met name natuurlijk over het belangrijke onderwerp online veiligheid en cybersecurity. Ik weet dat aan het begin de opmerking gemaakt werd dat er niet zo heel veel Kamerleden zijn en dat we dus wat meer tijd hebben om erover te spreken. Ik zag net een foto van alle ambtenaren die in een zaal hier heel ver vandaan wel zitten en heel hard werken voor al deze antwoorden van verschillende ministeries bij elkaar. Het is misschien ook mooi om aan te geven dat daar heel veel mensen integraal met elkaar druk mee bezig zijn. Normaal gesproken natuurlijk ook, maar ook op dit moment.
Voorzitter. De afgelopen periode heeft de noodzaak van een digitaal veilige samenleving alleen maar verder onderstreept. De verhoogde dreiging vanuit de oorlog in Oekraïne geeft een extra reden om de digitale veiligheid op orde te hebben; ik kom daar straks natuurlijk op terug. Niet eerder is zo duidelijk sprake geweest van een hybride oorlogvoering. Er is sprake van desinformatiecampagnes en er vinden digitale aanvallen plaats. We zien bijvoorbeeld dat websites van onder meer overheidsinstel-

lingen in Oekraïne en Rusland de afgelopen periode regelmatig plat zijn gelegd door cyberaanvallen.
In Nederland zien we nog geen aanzienlijke toename van digitale incidenten, maar we moeten ons hier natuurlijk wel op voorbereiden, en voorbereid zijn. Als coördinerend Minister voor cybersecurity is het mijn taak om het almaar groter wordend belang van digitale veiligheid en weerbaarheid te agenderen. Ik ben blij dat dit ook hier gezamenlijk in deze commissie kan. Het lijkt me dus ook een heel goede kans om dit op deze manier samen op te pakken.
Voorzitter. COVID-19 heeft ervoor gezorgd dat de digitalisering van onze maatschappij in een stroomversnelling kwam. We werken digitaal, we winkelen digitaal, we ontmoeten elkaar digitaal. Digitale systemen vormen inmiddels spreekwoordelijk het zenuwstelsel van onze maatschappij. Kortom, onze samenleving en economie zijn vrijwel volledig verweven met de digitale wereld. De veranderende geopolitieke verhoudingen, de continue technologieontwikkeling en de afhankelijkheid van digitale systemen brengen enorme kansen, maar ook grote risico's met zich mee.
Er is bijvoorbeeld sprake van een aanhoudende stroom van ransomware-aanvallen; daar werden ook wat vragen over gesteld. Dat zijn natuurlijk hacks met als doel om hier losgeld voor te krijgen. We zien de laatste jaren bijvoorbeeld een nieuwe trend ontstaan waarbij kwaadwillenden steeds meer gerichte ransomware-aanvallen uitvoeren op doelwitten die een hoger losgeldbedrag kunnen betalen.
Digitale kwetsbaarheden kunnen grote risico's met zich meebrengen. Denk bijvoorbeeld aan de kwetsbaarheid die eind vorig jaar werd ontdekt in de software Log4J. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Door het incident hebben verschillende organisaties zoals de Kamer van Koophandel en banken hun systemen tijdelijk uitgeschakeld om misbruik te voorkomen. Hierbij werd duidelijk dat het voor veel organisaties buitengewoon lastig is om na te gaan of zij en hun leveranciers Log4J in gebruik hadden en wat de gevolgen van misbruik van deze kwetsbaarheid precies zouden zijn. Tot nu toe is de schade beperkt gebleven. Misbruik van deze kwetsbaarheid had potentieel tot zware economische en maatschappelijke gevolgen kunnen leiden. Dat risico is nog niet voorbij.
Voorzitter, ik heb iets meer tekst dan ik normaal uitspreek bij een inleidende tekst – ik ben bijna klaar, hoor – omdat daarmee niet alleen de urgentie van wat er nu gebeurt, maar ook datgene wat we hebben opgetuigd enigszins bij elkaar komen. Daarna kom ik concreet op alle vragen terug.
Het Nationaal Cyber Security Centrum heeft in toenemende mate te maken met incidenten waarbij misbruik in potentie heel grote schade kan veroorzaken.
Voorzitter. Dit zijn een aantal dreigingen en ontwikkelingen. We kunnen daar nog heel lang over doorgaan, maar dit laat zien hoe urgent het onderwerp is en hoe relevant het is dat we het blijvende belang van cybersecurity en de noodzaak van passend overheidsbeleid onderstrepen. Cybersecurity is een randvoorwaarde voor een veilige en steeds meer digitaliserende maatschappij geworden. Daarom werkt het kabinet aan een nieuwe Nederlandse cybersecuritystrategie. Ik heb al heel veel mooie ideeën daarvoor genoemd. Toen we zojuist alle vragen doornamen, werd mij door de ambtenaren die daar nu al heel druk mee bezig zijn, gezegd: wat mooi dat alle input naadloos aansluit bij deze strategie en hoe we het zouden willen zien, ook vanuit de inhoud. Ik denk dat we elkaar daarin hopelijk heel snel kunnen vinden.
Voorzitter. De nieuwe strategie zal een aantal bekende knelpunten adresseren, zoals op het gebied van informatie-uitwisseling. Ik kan daar nog langer op doorgaan, maar ik kom op de vragen hierover straks terug. Wellicht is het nog wel goed om het volgende aan te geven. We zitten er

nu mee dat sommige informatie bedrijfsvertrouwelijk is of privacygevoelige data kan bevatten. Daarom kan niet altijd alle relevante informatie met iedereen gedeeld worden; in verschillende inbrengen kwam dit ook terug. Die informatie wordt bij dat soort incidenten en gevallen op het moment dat het noodzakelijk is, gedeeld met de rijksoverheid en vitale sectoren. Dat gebeurt door ... Er was natuurlijk heel veel behoefte om hiervoor een landelijk dekkend stelsel te hebben. Dat moet ook in de strategie plaatsvinden. Waarom? Omdat je zo veel mogelijk partijen wilt kunnen bereiken op het moment dat er iets aan de hand is. We hebben in dit verband vorig jaar zomer wel een wijziging van de Wet beveiliging netwerk- en informatiesystemen in procedure gebracht. Dat voorstel voorziet in een ruimere bevoegdheid voor het Nationaal Cyber Security Centrum. Dat is natuurlijk bedoeld om relevante dreigings- en incidentinformatie breder te kunnen delen. Dat is nog even goed om te benadrukken; daarna ga ik naar de mapjes. Het voorstel wordt deze maand nog bij de Tweede Kamer ingediend. Gezien de noodzaak van deze ruimere bevoegdheid maak ik ook graag gebruik van dit moment om dit extra te onderstrepen. Ik wil een dringende oproep aan de Kamer doen om daar als het kan met hoge prioriteit kennis van te nemen en actie op te ondernemen, zodat we dit spoedig kunnen behandelen. Hier is namelijk echt heel veel behoefte aan.
Ik stel voor dat ik mijn mooie afronding oversla en dan naar de mapjes ga. Ik vind namelijk dat ik zelf te lang aan het woord ben met een inleidende tekst. De mapjes die ik heb, gaan over de volgende onderwerpen. Informatie delen en stelsel. Strategie en de middelen uit het coalitieakkoord. De incidenten en wat er nu aan de hand is tussen Rusland en Oekraïne. Encryptie. En dan het mapje overig.
Ik begin met het onderwerp informatie delen. Van verschillende partijen, volgens mij ook van D66, kwam de volgende vraag. We zien een toename in ransomware en hacks; hoe zorgen we ervoor dat het bedrijfsleven deze urgentie ook ziet en op korte termijn handelingsperspectief heeft? Je wilt namelijk dat iedereen alert is. Je wilt informatie kunnen delen met degenen die die informatie moeten hebben, maar je wilt ook dat iedereen alert is en alles aan heeft staan om snel te kunnen handelen.
Ik ga proberen om heel veel afkortingen te vermijden, voorzitter. Soms gaat het niet lukken, want dit is volgens mij de commissie waarbij geldt: als je geen afkorting gebruikt, heb je niet geleefd. Het NCSC en het DTC, het Digital Trust Center, werken nauw samen om ervoor te zorgen dat ook het bedrijfsleven een handelingsperspectief kan hebben. Zij zijn voortdurend bezig met het ontwikkelen van manieren om meer informatie te kunnen delen en ze zijn ook met de NCTV in gesprek over het delen van informatie binnen het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden. Zij zijn hier ook mee bezig richting de ontvangers, en dat is net zo belangrijk, zodat zij daar ook een handelingsperspectief aan kunnen verbinden. Je kunt wel informatie krijgen, maar als je vervolgens niet weet wat je daarmee moet doen, helpt dat nog steeds niks. Alleen als we dat allemaal zo hebben georganiseerd en ook die alertheid hebben, kun je de digitale weerbaarheid verhogen in ons hele land en bij iedereen bij wie dat nodig is.
Het Digital Trust Center heeft sinds juni dit jaar tot eind 2021 bij vijftien cybersecurityincidenten dreigingsinformatie inclusief handelingsperspectief gedeeld met in totaal 361 niet-vitale bedrijven. Naast deze notificaties vindt bij het DTC momenteel een pilot plaats om bedrijfstechnische gegevens te matchen met dreigingsinformatie die bij de overheid bekend is. Om een match te kunnen maken, delen bedrijven vooraf vrijwillig hun technische gegevens met het DTC. Op het moment dat zij dat doen, kan het DTC daar vervolgens weer op handelen. Aan deze pilot nemen op dit moment 57 bedrijven deel. Ik denk dat het heel belangrijk is dat je op deze manier steeds verder ontwikkelt hoe je dit wilt vormgeven. Op vrijdag 15 oktober 2021 is het eerste pilotbedrijf genotificeerd door het

DTC over een aantal kwetsbaarheden die raakten aan meerdere systemen van het desbetreffende bedrijf. Door deze samenwerkingsvorm met het DTC en het NCSC kan snel en efficiënt dreigingsinformatie tussen bedrijven en de overheid worden uitgewisseld.

De heer **Bontenbal** (CDA):
De Minister noemt 57 bedrijven. Kan zij zeggen wat voor type bedrijven dat zijn?

Minister **Yeşilgöz-Zegerius**:
Ik ga checken of ik dat kan zeggen. Zo ja, dan kom ik daar in tweede termijn even op terug als dat oké is.

Mevrouw **Rajkowski** (VVD):
Als de Minister dan toch onderbroken is, had ik ook nog een interruptie staan. 361 bedrijven, dat klinkt aan de ene kant als heel veel, maar we hebben 2 miljoen bedrijven in Nederland. Voor zover ik begrepen heb, stond de teller in januari op 300. Moet ik dit dan zo interpreteren dat er sinds januari maar 60 of 61 bedrijven bij zijn gekomen?

Minister **Yeşilgöz-Zegerius**:
Ik ga die data ook checken. Daar kom ik zo ook op terug.

De **voorzitter**:
Oké. U kunt vervolgen.

Minister **Yeşilgöz-Zegerius**:
Dan had ik een vraag van mevrouw Van Ginneken, namelijk hoe de Wet bevordering digitale weerbaarheid bedrijven gaat helpen en waarom deze is vertraagd. Dit wetsvoorstel heeft tot doel de wettelijke basis te verstevigen van het Digital Trust Center, onder verantwoordelijkheid van het Ministerie van EZK, om operationele informatie over digitale dreigingen en kwetsbaarheden te ontvangen, te verwerken en te delen met bedrijven. Dat is een heel nuttige functie en tool, moet ik zeggen. Het Digital Trust Center richt zich op circa 2 miljoen, zoals mevrouw Rajkowski ... Hoe spreek ik dat eigenlijk uit? Een beetje jammer dat ik dat langs deze weg moet vragen, maar toch fijn dat ik het nu weet. Het Digital Trust Center richt zich op circa 2 miljoen niet-vitale bedrijven. Deze wet zal ervoor zorgen dat informatie sneller en gemakkelijker kan worden gedeeld tussen overheid en bedrijfsleven, in een landelijk dekkend stelsel. Dat vergemakkelijkt dat dus. Het wetsvoorstel Bevordering digitale weerbaarheid zal door de Minister van EZK op korte termijn worden aangeboden. Volgens mij is het al aangeboden aan de Raad van State. Er is heel veel input op gekomen vanuit de Raad van State, omdat het natuurlijk ook een heel brede wet is. Juist vanwege die input – zo moet ik het zeggen – is die vertraagd. Dat is de volgorde der dingen geweest.

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

Mevrouw **Van Ginneken** (D66):
Dank aan de Minister voor dit antwoord. Kan de Minister al iets zeggen over de aard van de opmerkingen die de Raad van State heeft gemaakt?

Minister **Yeşilgöz-Zegerius**:
Nee, dat kan ik niet. Dat ligt echt bij EZK. Wat ik wel kan doen, is deze vraag doorgeleiden naar mijn collega. Wellicht helpt dat. Dan zal ik aangeven dat daar in ieder geval een reactie op moet komen, of voor een debat op korte termijn of op een andere manier.

Dan vroeg mevrouw Rajkowski of er een algemeen keurmerk kan worden ontwikkeld voor mainports. Dat is een heel goede vraag. We zijn in Europees verband bezig om te kijken of dat mogelijk is en hoe dat er eventueel uit zou kunnen zien. Dus ik kan er nog niet ja of nee op zeggen, maar ik begrijp wel heel erg waar zij naar op zoek is. Ten aanzien van keurmerken voor ICT-producten en -diensten is het ook van belang dat maatregelen in de EU tot stand komen, omdat fabrikanten en leveranciers van dit soort producten en diensten, en grote afnemers veelal internationaal opererende bedrijven zijn. Dus daar kijken we op die manier naar. U heeft eind vorig jaar ook een non-paper ontvangen van de Minister van EZK over de EU-certificeringsschema's, ontwikkeld voor ICT-producten, -diensten en -processen, en het proces daaromtrent. Wij maken ons nu sterk voor een zorgplicht voor ICT-fabrikanten en leveranciers in de vormgeving van de Europese Cyber Resilience Act. Die wordt dit najaar verwacht. EZK heeft daar vorig jaar ook het een en ander over gezegd. Dus dat wordt allemaal goed uitgezocht in Europees verband.

Mevrouw **Rajkowski** (VVD):
Fijn om dit te horen en dank ook daarvoor. Inderdaad, de digitale snelweg houdt niet op bij de Nederlandse grens. Heel fijn dat Nederland er ook in Europees verband input op levert. Al die verschillende wet- en regelgeving gaat mijns inziens meer over losse producten, losse diensten en losse bedrijven. De VVD ziet graag dat we ook kijken ... Kijk bijvoorbeeld naar de Rotterdamse Haven. Daar zitten ook mkb'ers met misschien heel weinig werknemers, die je normaal misschien niet aan heel strenge eisen zou willen laten voldoen, maar omdat die mkb'ers in de Rotterdamse Haven zitten, waar je geen terminals wil laten stilleggen, moeten ze misschien wel aan die regels voldoen. Dat is dan dus ook meer gebieds- en functiegericht, naast dienst- en productgericht. Denk aan een keurmerk, überhaupt omdat je in een mainport zit en de impact dan groot is.

Minister **Yeşilgöz-Zegerius**:
Volgens mij kunnen we dit op deze manier goed meenemen, want dit gaat én over producten én over diensten én over afnemers. Volgens mij is dat ook de hele insteek van de vraag, namelijk om breed te kijken wat er in zo'n mainport gebeurt. We bekijken inderdaad op Europees niveau hoe je die beter kunt beschermen.
Dan heb ik hier een vraag van onder andere de PVV en ik meen ook van D66: zou het NCSC ook niet-vitale organisaties moeten bedienen? Het NCSC is op dit moment natuurlijk het nationale knooppunt in het landelijk dekkende stelsel van cybersecuritysamenwerkingsverbanden. Het richt zich primair op het Rijk en vitale sectoren. Het werkt samen met partners en schakelorganisaties, zoals het Digital Trust Center – dat richt zich dan weer op niet-vitale bedrijven – of Z-CERT, voor de zorg. Momenteel werkt het kabinet onder mijn coördinatie, die van mijn departement, aan een nieuwe integrale Nederlandse cybersecuritystrategie. Daarin komen verschillende stelselvraagstukken aan de orde. Daar is dit echt onderdeel van. Er wordt nu hard over nagedacht. Ik begrijp de vraag. Ik zou ook geneigd zijn om te zeggen dat het er in essentie wel onder moet vallen. Maar we zijn dit in die strategie nu precies aan het afwegen en aan het bekijken: als het ja is, hoe dan? Dan hebben we daar ook een ronder verhaal over. Dus in essentie lijkt het mij wel, maar we nemen het mee in het vormgeven van de strategie.

De **voorzitter**:
Een vraag tussendoor: is er ook een tijdlijn voor die strategie?

Minister **Yeşilgöz-Zegerius**:
Ja, voor de zomer.

De **voorzitter**:
Voor de zomer.

Minister **Yeşilgöz-Zegerius**:
Nou, dat is best snel.

Mevrouw **Van Ginneken** (D66):
Even een verduidelijkende vraag. Volgens mij hoor ik de Minister zeggen: in essentie koersen we af op het meer onder één dak brengen, of misschien wel helemaal onder één dak brengen van deze bevoegdheden om de digitale weerbaarheid van onze samenleving te borgen. Dus die beweging is eigenlijk al een genomen afslag, precies zoals ik ook voorstelde. Dus even de checkvraag: heb ik dat goed begrepen? Bekijkt de Minister alleen nog in welke vorm en met welke stappen we dat gaan doen en gaan we dat teruglezen in de genoemde strategie?

Minister **Yeşilgöz-Zegerius**:
Min of meer. Echt onder één dak brengen en de bevoegdheden samenvoegen: zo zou ik het nog niet willen invullen. Maar we kijken wel welke verschillende modellen hiervoor mogelijk zijn. Wat zijn de voor- en nadelen? Dat verkennen we met elkaar. Daar zitten we nu middenin. Dus de beweging en de behoefte zijn helder. Die zijn heel erg herkenbaar. Vervolgens moet je kijken hoe dat eruit zou kunnen zien en wat daar de voor- en nadelen van zijn, zodat we dan met elkaar kunnen beoordelen of het inderdaad helemaal die richting is of dat je er een paar stappen voor moet zetten om die samenwerking beter te maken. Dus min of meer wel, maar nog niet zo stellig als mevrouw Van Ginneken het zegt.
Door?

De **voorzitter**:
Ja. Ik zou vanuit de PVV aan willen geven dat het ook heel erg behulpzaam zou zijn dat er, als wij die nieuwe plannen ontvangen, ook een soort stroomschema of een organogram of iets dergelijks bij zit, zodat we op die manier visueel inzichtelijk krijgen wat het nieuwe stelsel dan is of wordt.

Minister **Yeşilgöz-Zegerius**:
Helemaal eens. Dat zou mij ook erg helpen. Dus dat lijkt mij een heel goed idee.
Ik was bij de heer Bontenbal. Hij stelde een heel fundamentele en terechte vraag, namelijk: zijn onze vitale sectoren voldoende weerbaar tegen digitale dreigingen? Dat is nu heel actueel, maar het was eigenlijk al die tijd al heel actueel. Het is uiteraard van groot belang dat vitale processen, zoals drinkwater en energie, ongestoord kunnen functioneren. Een goede digitale beveiliging is, zoals gezegd, cruciaal. In het Cybersecuritybeeld Nederland is de afgelopen jaren aangegeven dat de weerbaarheid soms achterblijft bij de toename van de dreiging. Cybersecurity is in de eerste plaats uiteraard een verantwoordelijkheid van de bedrijven zelf. Bescherm jezelf goed. Maar het mag niet vrijblijvend zijn, zeker niet vanuit onze rol als overheid, en zeker niet bij vitale processen. Daarom is er de afgelopen jaren heel veel werk van gemaakt. Vitale aanbieders hebben bijvoorbeeld sinds 2018 een zorgplicht, waarmee ze verplicht zijn om beveiligingsmaatregelen te nemen. Daarnaast geldt er een meldplicht voor incidenten, onder andere bij het Nationaal Cyber Security Centrum. Toezichthouders zien ook echt toe op de naleving van deze verplichtingen. Als gevolg van nieuwe Europese regelgeving zullen deze verplichtingen worden uitgebreid naar meer aanbieders, bijvoorbeeld in de zorgsector en in de voedingsindustrie. Naar verwachting zullen deze maatregelen in 2024 zijn omgezet in nationale wetgeving. Dus het blijft cruciaal om hieraan aandacht te besteden, denk ik.

Dan was er een vraag over de Wet beveiliging netwerk- en informatiesystemen, volgens mij van mevrouw Van Weerdenburg. Hoe ga ik haast maken? Wat is ervoor nodig? Het voorstel tot wijziging van deze wet zorgt ervoor dat het Nationaal Cyber Security Centrum met alle in de Wet beveiliging netwerk- en informatiesystemen aangewezen schakelorganisaties meer informatie kan delen en in bepaalde gevallen organisaties direct kan waarschuwen indien er geen schakelorganisatie aanwezig is. Het is nogal relevant dat we dit snel voor elkaar krijgen. Zowel de Autoriteit Persoonsgegevens als de Raad van State heeft inmiddels een advies over het wetsvoorstel uitgebracht. Het advies van de Autoriteit Persoonsgegevens is al in het voorstel verwerkt. Dat van de Raad van State wordt momenteel nog verwerkt. Wij verwachten het op korte termijn, deze maand nog, bij de Tweede Kamer in te dienen. Het zal in ieder geval niet aan ons liggen. We werken er hard aan om het hier te hebben liggen. Ik hoop dat er in de tussentijd niet nog iets extra's nodig is en dat die al vrij snel hier ligt. Daarmee delen we de urgentie op dit onderwerp. Dus wij doen ons best. Het zal niet aan ons liggen.

De **voorzitter**:
De oproep is genoteerd.

Minister **Yeşilgöz-Zegerius**:
Dat is fijn. In het verlengde hiervan was er nog een vraag van mevrouw Van Ginneken. Zij vroeg hoeveel extra werk dit is, bijvoorbeeld voor de Autoriteit Persoonsgegevens. Wat komt hier nog achter weg? De wijzigingen brengen geen nieuwe grondslag voor verwerkingen met zich mee. Dat is dus een relevante opmerking. Op het moment van het schrijven van de wet was het doel om eventuele restinformatie te delen met zogenoemde schakelorganisaties. Alleen, hierin is een zogenoemde OKTT ... Ik leg het even uit voor al die Nederlanders die nu naar ons kijken en die zeggen: wat is nou een OKTT? Dat zijn organisaties die objectief kenbaar tot taak hebben om organisaties of het publiek te informeren over dreigingen en incidenten. Daarin was de zogenoemde OKTT niet meegenomen als schakelorganisatie die alle informatie ontvangt. Dat is een weeffout. Met het wetsvoorstel wordt die hersteld. De wetswijziging brengt wel met zich mee dat er meer persoonsgegevens verwerkt zullen worden, maar naar verwachting levert dit geen grotere toezichtlast op voor de Autoriteit Persoonsgegevens. Naar deze vraag is dus expliciet gekeken.
Dan ben ik bij het mapje strategie en de coalitieakkoordmiddelen. Er was een vraag van de VVD en D66 over het Digital Trust Center. Past de huidige rolverdeling tussen NCSC en DTC nog? Hoe zit dat eigenlijk? Kunnen ze dichter bij elkaar gebracht worden? Volgens mij heb ik die vraag trouwens ook van andere partijen gehoord. Het Nationaal Cyber Security Centrum is onderdeel van het Ministerie van Justitie en Veiligheid en werkt aan een digitaal veilig Nederland. Het Ministerie van EZK heeft in 2018 het Digital Trust Center opgericht om de 2 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Het Nationaal Cyber Security Centrum en het Digital Trust Center hebben ieder hun eigen primaire doelgroep. De rijksoverheid en vitale aanbieders worden bediend door het NCSC en het niet-vitale bedrijfsleven door het Digital Trust Center. Beide organisaties hebben doelgroepspecifieke kennis opgebouwd, waardoor zij in staat zijn om hun doelgroep zo goed mogelijk te bedienen.
Om deze doelgroepen te kunnen bedienen werken ze wel zeer nauw samen. Dat is dus heel erg terecht opgemerkt door iedereen die deze vraag heeft gesteld of hiernaar op zoek is geweest. Ze zijn voortdurend, samen met de NCTV, in gesprek over het delen van informatie binnen het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden. Zoals ik net ook zei, ben ik het er ontzettend mee eens dat we hier scherp

op moeten blijven en dat je niet wil dat deze partijen, die zo cruciaal zijn breed in de samenleving, naast elkaar werken. We moeten dus scherp blijven op de rolverdeling, de efficiënte inzet van de beschikbare capaciteit en de duidelijke rolverdeling richting de doelgroepen, en zorgen dat ze nauw samenwerken. Om deze vraagstukken allemaal goed in de gaten te kunnen houden en nog beter te kunnen borgen, wordt momenteel verkend hoe deze beide instanties nog intensiever kunnen samenwerken. Die uitkomsten zult u voor de zomer terugzien in de cybersecuritystrategie.
Dan was er een vraag van mevrouw Van Ginneken. Wat vindt de Minister van de conclusie van de Cyber Security Raad dat er meer dan 800 miljoen euro bij moet om onze cyberveiligheid te waarborgen? Misschien is het goed om van tevoren ...

De **voorzitter**:
Mevrouw Van Ginneken wil iets aanvullen?

Mevrouw **Van Ginneken** (D66):
Ik wil even iets checken, want ik heb de indruk dat de Minister nu overgaat naar het volgende blokje.

Minister **Yeşilgöz-Zegerius**:
Nee.

De **voorzitter**:
Het is nog hetzelfde blokje.

Minister **Yeşilgöz-Zegerius**:
In ons hoofd klonk dit heel logisch als één blokje.

Mevrouw **Van Ginneken** (D66):
Dit is allemaal het stelsel, waar we het nu over hebben?

Minister **Yeşilgöz-Zegerius**:
Ik was al bij het volgende blokje: strategie en coalitieakkoordmiddelen.

Mevrouw **Van Ginneken** (D66):
Kijk, dan was ik niet helemaal scherp. Ik had nog een vraag over het stelsel, want een van de vragen waarvan ik dacht dat die onder dat kopje vielen, is nog niet beantwoord. Dat is namelijk een specifieke vraag. Het NCC, dus het nationaal coördinatiecentrum, is in oprichting als gevolg van Europese regelgeving. Dat valt onder EZK, dus het raakt sowieso de hele discussie: zijn we het allemaal niet veel te veel aan het versnipperen? Mijn vraag aan de Minister was: waarom is die nieuw op te richten organisatie niet ondergebracht bij ofwel NCSC ofwel DTC?

De **voorzitter**:
Ja, want op dit moment wordt die organisatie ondergebracht bij de RVO? Ja.

Minister **Yeşilgöz-Zegerius**:
Ja. Ik heb hem voorbij zien komen. Volgens mij zit die in het onderste mapje, overig, dus als mevrouw Van Ginneken het goedvindt ... Als ik hem nu eruit ga vissen, raak ik door al die mapjes in de war. Oké, top, dan doen we hem zo. Als hij daar niet tussen zit, dan kom ik er sowieso straks op terug. Dank u wel.
Dan ben ik weer terug bij de 800 miljoen, ook van mevrouw Van Ginneken; althans, was het maar zo, maar bij de vraag. Zoals ik net wilde zeggen: dat bedrag vraagt wel om enige nuancering in hoe het is opgebouwd, want de Cyber Security Raad adviseert dat, maar er worden

daarbij voorstellen gedaan die zien op zowel cybercrime als cybersecurity, terwijl de investering van 150 miljoen daarbinnen bijvoorbeeld alleen is bedoeld voor cybersecurity. Daarnaast maakt de Cyber Security Raad geen onderscheid tussen structurele en incidentele investeringen, waardoor het uiteindelijke geadviseerde bedrag hoger uitvalt.
Hoe dan ook – het maakt niet uit – is dit heel belangrijk voor het digitaal weerbaar maken en houden van Nederland. Dat is een enorme opgave en daar zijn gewoon middelen voor nodig. Dat blijft, hoe dan ook, overeind staan. Het vorige kabinet heeft hierin een eerste stap gezet, met een investering van 93 miljoen op dit thema. We bouwen hierop voort met een investering van 150 miljoen, structureel. We hebben niet de illusie dat daarmee dan alles geregeld is. Zoals gezegd, kun je de opbouw van bepaalde bedragen en investeringen nuanceren of beter duiden, maar uiteindelijk zullen we de komende jaren aandacht moeten blijven besteden aan dit thema. We zullen met elkaar moeten volgen of er meer nodig is en zo ja, wat dan, waar dan en op welke plek dan? Ik denk dat we daar either way heel veel aandacht aan moeten blijven geven. Denk ook aan de samenwerking met private partners. Het coalitieakkoord biedt ons gelukkig ook wel enige ruimte om daar stappen in te zetten op dit moment.

Mevrouw **Van Ginneken** (D66):
Ik deel de observatie van de Minister dat in het rapport van de Cyber Security Raad inderdaad een breed pakket wordt neergelegd. Ik heb het er even bij gepakt. Er zijn vijf posten, waarvan ik er drie ga noemen die volgens mij echt met dit onderwerp te maken hebben. Regie op samenwerking informatiedeling: 92 miljoen. Weerbare vitale processen en infrastructuur: 218 miljoen. Handhaving en bescherming tegen cybercrime: 330 miljoen. Dat laatste is zo'n post waarvan je zegt: bescherming hoort hier misschien wel bij, maar handhaving is misschien een ander vraagstuk. Het zijn behoorlijk grote bedragen. Ik hoor de Minister zeggen: 93 miljoen van het vorige kabinet en 150 miljoen nu. Daar zit gevoelsmatig, nog los van de wat vage afspraken over die posten, een heel groot gat tussen. Cybersecurity is natuurlijk wel echt een heel belangrijk onderwerp om onze samenleving veilig en weerbaar te houden, zowel in democratisch en sociaal opzicht als in economisch opzicht. Ik zou de Minister dus willen uitdagen om nog iets specifieker te worden, zeker ook omdat ik de 150 miljoen die zij noemt niet kan teruglezen in de financiële paragraaf van het coalitieakkoord. Wat doen we nou precies en kan het niet een onsje meer?

De **voorzitter**:
En waar staat het?

Minister **Yeşilgöz-Zegerius**:
Voor het onsje meer moet u bij de onderhandelaars van het coalitieakkoord zijn, maar ik kan wel zeggen waar we nu voor staan. Het is misschien goed om het even specifiek te maken. De uitwerking komt ook nog naar de Kamer. Het kabinet zal dit jaar 60 miljoen extra investeren in cybersecurity. Dat zal oplopen tot 300 miljoen structureel vanaf 2027. Dat is de 300 miljoen die je terug kunt vinden in het coalitieakkoord. De afgelopen drie maanden – we zijn drie maanden bezig als nieuw kabinet – hebben we vooral met de inlichtingendiensten, de veiligheidsdiensten en de NCTV, alle diensten die bezig zijn met cybersecurity, gezamenlijk gekeken wat nou een zinnige verdeling is en waar extra inzet nodig is, in welke richting en bij welke posten, zoals mevrouw Van Ginneken voorlas uit het rapport van de Cyber Security Raad. Daarvoor lag er natuurlijk ook heel veel andere input.
De bel van de Tweede Kamer gaat, maar ik praat gewoon door, hoor.

De **voorzitter**:
U mag ook even pauzeren. Het is de stemmingsbel, dus dat is een lange. We hoopten allemaal op een mute button in het nieuwe gebouw, maar het mocht niet zo zijn. De Minister vervolgt haar betoog.

Minister **Yeşilgöz-Zegerius**:
Voorzitter. Ik was net aan het toelichten hoe die 300 miljoen op hoofdlijnen verdeeld lijkt te worden, maar het wordt sowieso, hopelijk voor de zomer, met de nieuwe strategie, nauwkeurig voor u op papier gezet en met u gedeeld. Daarna kunt u er natuurlijk nog van alles van vinden, maar ik noem wel een paar stappen, omdat daar vragen over zijn gesteld. Met dat geld wordt geïnvesteerd in onder andere de slagkracht van de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst, dus de AIVD en de MIVD, het Nationaal Cyber Security Centrum en het bredere beleidsterrein van economische veiligheid, cybersecurity en de vitale infrastructuur. Dat is heel bewust breed, maar gefocust aangevlogen. De investering op digitale veiligheid bedraagt rond de 150 miljoen. Een substantieel deel daarvan gaat naar de inlichtingen- en veiligheidsdiensten. Daarnaast wordt 33 miljoen geïnvesteerd in het Nationaal Cyber Security Centrum, 34 miljoen in de vitale infrastructuur en 54 miljoen in het bredere cyberdomein. Nogmaals, de uitwerking komt uiteraard naar u toe, met vanzelfsprekend een onderbouwing in relatie tot de strategie. Zoals gezegd is geprobeerd om een balans te vinden tussen operationele capaciteit bij de diensten en investeringen verderop in de keten, omdat je het risico wilt voorkomen dat je aan één kant heel erg investeert en de keten vervolgens aan de andere kant vastloopt. Het is een hele complexe opgave, want hadden we meer kunnen uitgeven, dan was het meer complex, en hadden we minder kunnen uitgeven, dan hadden we het nog ingewikkelder gehad. Er is een integrale benadering nodig om te kijken wat er echt nodig is en hoe je het maximale kunt doen met de middelen die je hebt om Nederland zo weerbaar mogelijk te maken.

De **voorzitter**:
Wellicht een suggestie van mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Laat ik niet zo aanmatigend zijn dat nu alvast meteen in te vullen, maar ik heb wel een vraag. Ik ben heel blij met deze opsomming. Ik heb het niet helemaal kunnen bijhouden, maar gelukkig kunnen we debatten terugkijken. Dat is altijd goed. Ik heb de Minister horen zeggen dat het ook in de cybersecuritystrategie wordt opgenomen. Dat is fijn. Ik ving wel op: 54 miljoen voor het NCSC. Het Cyber Security Raadrapport zegt: 92 miljoen. Daar zit een gat. Geld dat er niet is, kun je natuurlijk niet toekennen. Dat begrijp ik. Maar ik ben wel benieuwd – kan de Minister toezeggen daar ook in de strategie op in te gaan? – welk deel van de ambities van het NCSC we dan niet kunnen invullen en waar het geld dan prioritair wel en niet aan wordt besteed, zodat we daar meer zicht op hebben en daarop kunnen sturen.

Minister **Yeşilgöz-Zegerius**:
Het was zelfs 33 miljoen voor het NCSC, dus dan maak ik het verhaal nog ietsje ... Maar inderdaad, we zullen daar natuurlijk duidelijk in opnemen wat de ambities zijn, wat de strategie is, wat de huidige doelen zijn en wat je hiervoor kan doen, en vanzelfsprekend wat je hiervoor dan niet kan doen, maar dat wordt vanzelf duidelijk als je het voorgaande goed hebt onderbouwd.
Dan was er nog een vraag over de Europese samenwerking. Von der Leyen riep op tot het bundelen van cybercapaciteit. Hoe kan Nederland hier een leidende rol in spelen? Dat is een terechte vraag, want cyberdreigingen houden zich uiteraard niet aan landsgrenzen, dus is internationale

en Europese samenwerking cruciaal. Nederland is dan ook blij dat de Europese Commissie hier veel aandacht aan besteedt met de Europese cybersecuritystrategie die eind 2020 is gepubliceerd. Nederland stelt zich in Europese besprekingen op als een voorstander van goede Europese samenwerking op cybersecurity, ook als het gaat om het versterken van bestaande netwerken. Een voorbeeld daarvan is het CyCLONe-netwerk, dat is gericht op samenwerking in geval van een cybercrisis. Zo heeft Nederland bijvoorbeeld een Europese strategische oefening georganiseerd in 2020, waar dit netwerk ook is gelanceerd. Dat laat goed zien welke rol Nederland daarin speelt. Daarnaast zijn we natuurlijk een van de lidstaten die actief bijdraagt aan de rapid response teams binnen PESCO. Dat staat voor Permanent Structured Cooperation. We zijn een van de lidstaten die daar een actieve rol in speelt. Uiteraard blijft Europese samenwerking in de komende jaren erg relevant. In de Nederlandse cybersecuritystrategie zullen we ook nader ingaan op wat de internationale samenwerking nog meer zou kunnen zijn.
Dan ben ik bij concrete incidenten. Ik heb er zelfs bij staan «Rusland», maar dat is natuurlijk het meest actuele. Daar waren ook een aantal vragen over. Ik heb hier als eerste een vraag van de PvdA. Mevrouw Kathmann zei over Kaspersky: waarom ook niet bij andere producten? Hoe zat dat precies? In 2018 heeft het kabinet bepaald dat als voorzorgsmaatregel Kaspersky antivirussoftware bij de rijksoverheid wordt uitgefaseerd. Aan bedrijven en organisaties met vitale diensten en processen en aan bedrijven die vallen onder de Algemene Beveiligingseisen voor Defensieopdrachten, de zogenaamde ABDO, is geadviseerd om hetzelfde te doen. Deze maatregel werd genomen met het oog op het waarborgen van de nationale veiligheid. Het was een combinatie van factoren die in deze casus ertoe hebben geleid dat er sprake was van risico's voor de nationale veiligheid, die het kabinet waar mogelijk wilde voorkomen. Onderdeel van de afweging was de Russische wetgeving, die bedrijven als Kaspersky verplicht samen te werken met de Russische overheid. De antivirussoftware zit diep in de systemen en kan bij misbruik een groot veiligheidsrisico vormen. Gericht op de vraag van mevrouw Kathmann: het is altijd een afweging waarbij je al dit soort factoren meeweegt. Je kijkt waar de te beschermen belangen zitten, wat je kan monitoren, wat je kan zien en waar je nauwelijks zicht op hebt. Naar die afweging kijken we altijd heel kritisch. Maar hier waren nogal duidelijke factoren waardoor de overheid heeft gezegd: dit gaan we uitfaseren. Dus als zo'n afweging bij andere zaken zou gelden, dan zou dat kunnen. De vraag was: waarom hierbij? Om die reden dus.

De **voorzitter**:
Mevrouw Kathmann, volgens mij had u ook gevraagd: waarom antivirussoftware wel en de rest niet?

Mevrouw **Kathmann** (PvdA):
Ja, dat was de vraag vooral. Waarom is ervoor gekozen om alleen de antivirussoftware uit te faseren en niet de andere producten?

Minister **Yeşilgöz-Zegerius**:
Die antivirussoftware zat heel diep in de systemen. Er was dus een groot risico op misbruik. Ik kan even kijken of we er in tweede termijn nog nader op in kunnen gaan, maar dat was een van de meest concrete redenen om het hier wel bij te doen, omdat het risico op andere gebieden minder was. Ik zal even kijken of ik er in tweede termijn nog nader op in kan gaan, maar het zal ongeveer een dergelijk antwoord zijn. Maar ik ga graag kijken of ik één slag dieper kan.

Mevrouw **Kathmann** (PvdA):
Een beetje gezien de actualiteit, omdat het gaat over rijksoverheid en vitale bedrijven. Het zijn ABDO-bedrijven, toch? Al die leuke afkortingen. Gezien de actualiteit vraag ik me af wat nu de stand van zaken is. Geldt dan nog steeds dat ook deze vitale spelers producten van Kaspersky Lab kunnen overnemen, als het maar geen antivirussoftware is?

Minister **Yeşilgöz-Zegerius**:
Ik begrijp de relevantie van de vraag. Ik kijk of ik in tweede termijn daar een slag dieper op in kan gaan. Zo niet, dan vinden we een andere oplossing.
Dan vroeg mevrouw Rajkowski of ik kan reageren op het feit dat Russische hackers vrijelijk aanvallen kunnen uitvoeren. Kunnen deze hackers niet op een sanctielijst geplaatst worden? De aanval op de woningcorporaties, zeer actueel, laat wederom zien dat ransomware een enorm impactvol delict is dat behoorlijk veel consequenties heeft. Daarbij komen slachtoffers ook enorm onder druk te staan. Het lijkt soms iets abstracts, omdat je het niet ziet gebeuren. Er staan niet iemand met een bivakmuts en een pistool voor je neus, maar het is zeer impactvol. Er is niet alleen sprake van financiële schade, maar criminelen publiceren ook gevoelige gegevens en kunnen er daarna weer van alles mee doen. Ik heb er groot respect voor dat de woningcorporaties geen losgeld hebben betaald. Dat zal vast niet een heel makkelijke afweging zijn geweest. Maar het helpt echt wel bij het tegengaan van dit delict, hoe lastig het dan ook is, omdat de gevolgen daarvan ook weer groot kunnen zijn. De politie is op de hoogte van deze specifieke zaak en is ook bekend met de ransomwaregroeperingen die dit soort aanvallen uitvoeren. De politie doet onderzoek naar ransomwareaanvallen en de groeperingen die erachter zitten. Ik denk dat het heel belangrijk is om hier expliciet bij stil te staan. Daarom noem ik het nadrukkelijk, hoewel ik weet dat de vraag van mevrouw Rajkowski breder was. Het is goed om hier expliciet bij stil te staan, omdat hackers die dit soort aanvallen uitvoeren enorm veel geld kunnen verdienen en er ook gewoon mee weg kunnen komen. Dus de politie zit hier echt bovenop om te voorkomen dat internet een vrijplaats wordt voor criminelen. De Kamer is uiteraard al eerder geïnformeerd over hoe complex opsporing in het digitale domein is, maar er wordt dus hard aan gewerkt.
Het is misschien goed om over te gaan naar de vraag over de sanctielijst. Dit waren vragen die in elkaars verlengde lagen. Het Ministerie van Buitenlandse Zaken heeft aangegeven bereid te zijn om te kijken of er voor deze casus mogelijkheden zijn om EU-sancties op te leggen. Dat wordt onderzocht. Het is wel nodig dat we voldoende concrete informatie hebben om daarop te kunnen handelen. Ik noem dat er even bij, omdat het daarom op dit moment nog erg vroeg is om conclusies te trekken over de haalbaarheid hiervan, of om die in te kunnen schatten. We hebben informatie nodig over de aard en de impact van de aanval. We moeten duidelijk krijgen wie er achter de aanval zit en of er vervolgens EU-sancties mogelijk zijn. Dat hangt ook weer af van de steun van andere lidstaten. Maar we zijn dus zeker bereid om naar deze casus te kijken. Dat wordt ook opgepakt.
Deze vraag is van mevrouw Van Ginneken. De Amerikaanse president, Biden, waarschuwde dat Rusland van plan is wraak te nemen op iedereen die Oekraïne digitaal steunt. Dat zou forse gevolgen kunnen hebben voor Nederland. Wat doen we om de risico's te beperken? Het Nationaal Cyber Security Centrum houdt sinds het begin van de spanningen alle ontwikkelingen omtrent de situatie in Oost-Europa nauwlettend in de gaten. Hun observatie is dat de dreiging sinds het uitbreken van de oorlog wel groter is geworden. Zij houden dan ook op korte termijn rekening met nieuwe aanvallen die te relateren zijn aan deze oorlog. Deze aanvallen kunnen ook, zoals terecht gesteld, impact hebben op Nederland. Dat kan gaan

over gerichte aanvallen op Nederland, bijvoorbeeld als vergelding van sancties zoals waar we het zojuist over hadden. Dat kan. Nederlandse instellingen kunnen onbedoeld doelwit worden van een aanval en Nederlandse digitale infrastructuur kan misbruikt worden voor het uitvoeren van digitale aanvallen. Daar heb ik ook eerder Kamervragen over gezien. Op dit moment is het wel goed om te benadrukken dat we ons bewust zijn van de risico's. Het wordt in de gaten gehouden, maar op dit moment hebben we geen concrete aanwijzingen dat er gerichte digitale aanvallen op Nederland hebben plaatsgevonden.
De verhoogde dreiging vanuit de oorlog in Oekraïne geeft wel een extra reden om de digitale veiligheid op orde te hebben en alert te blijven. Om de risico's in de samenleving te beperken is de afgelopen weken ook door het NCSC en de NCTV extra nadruk gelegd op het belang van cyberweerbaarheid en waakzaamheid. Daar is heel veel aandacht aan besteed. Het NCSC biedt daarvoor samen met het Digital Trust Center openbare webinars en houdt een informatiepagina bij op zijn website. Ik heb ook van verschillende betrokkenen begrepen dat daar dankbaar gebruik van wordt gemaakt. Er is natuurlijk heel veel behoefte aan wat tools om te weten «waar ben ik aan toe» en «hoe kan ik mezelf goed beschermen». Zo heeft het Digital Trust Center in samenwerking met het NCSC het webinar Oorlog in Oekraïne en digitale veiligheid in Nederland georganiseerd. Dat ging over een update van het dreigingsbeeld en digitale aanvalstechnieken voor onze doelgroepen. Ook eerder, 9 maart al, gaf het een online informatiesessie met als titel Huidig beeld en digitale impact van de oorlog in Oekraïne. Dan heb je bijvoorbeeld 144 vragen tijdens zo'n webinar. Dat zijn hele gerichte vragen als «hoe kan je me hierbij helpen». Die komen van de bijna 4.000 bezoekers die dat webinar op dat moment bekeken. Iedereen die online weleens wat heeft georganiseerd weet dat dit forse getallen zijn. Dat laat zien dat er heel veel behoefte aan is. Daar wordt ook volop aandacht aan besteed.

Mevrouw **Van Ginneken** (D66):
U vroeg mij zojuist bij een interruptie, een andere vraag, of ik een goed voorstel had. Ik zou hier eigenlijk nog wel een voorstel willen doen aan de Minister. Ik ben blij om te horen dat er geen concrete aanwijzingen zijn dat aanvallen uitgevoerd zijn of worden. Het is ook fijn om te horen dat er ingezet wordt op bewustwording en kennisdeling, maar we weten allemaal dat veel hacks en ransomwareaanvallen gebruikmaken van allang bekende kwetsbaarheden in systemen. Soms gaat het om een nieuwe, onbekende kwetsbaarheid, maar vaak zijn ze bekend en kunnen hackers er gebruik van maken omdat systemen niet up-to-date zijn. Dat heeft soms te maken met gebrek aan aandacht van de organisaties die dat zouden moeten doen in hun eigen systemen, maar soms ook met gebrek aan capaciteit. Ziet de Minister daar niet een oplossing om bijvoorbeeld middelen vrij te maken om een patchbrigade door Nederland te sturen om alle bedrijven die nog niet helemaal up-to-date zijn met patches daarbij te helpen? Kan de Minister toezeggen daar eens naar te kijken?

De **voorzitter**:
De patchpolitie. De Minister.

Minister **Yeşilgöz-Zegerius**:
De vraag begon met «middelen vrijmaken». Dan heb geleerd als Kamerlid, maar ook als bewindspersoon, dat ik even alert moet zijn. Ik vertelde net dat ik geen middelen heb, maar ik begrijp de vraag wel. In de basis is het denk ik goed dat we één ding niet uit het oog verliezen, namelijk dat het primair de eigen verantwoordelijkheid is, want anders lukt het nooit om de digitale weerbaarheid waar we zo naar op zoek zijn in het hele land te realiseren. Daarom is het zo belangrijk dat je dingen juist zo breed mogelijk organiseert, zoals ik net zei over de bijna 150 gerichte vragen van

4.000 bezoekers, zodat partijen zelf aan de slag kunnen. Persoonlijk denk ik dat dat effectiever is, ook in deze tijd, waarin je weet dat er gewoon een hoge mate van paraatheid nodig is. Er is verhoogde dreiging. Dit is denk ik sneller. Er is een sterke toename van het aantal bezoeken aan de Basisscan Cyberweerbaarheid. Dat stijgt hard. Er is hier echt behoefte aan. Mensen reageren er ook echt op en gaan er vervolgens mee aan de slag. We kunnen er inhoudelijk naar kijken als mevrouw Van Ginneken zegt: «Ik heb een concreet voorstel. Dat ga ik indienen. Hierin kan je zien wat het betekent.» Maar ik zou zeggen: laten we de capaciteit die we hebben ook op deze manier met een zo breed mogelijk bereik blijven organiseren, zodat die eigen verantwoordelijkheid – dat is makkelijk gezegd, maar je moet maar weten waar je aan toe bent – echt ingevuld kan worden. Dat zou op dit moment mijn antwoord zijn.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter, voor uw coulance qua interrupties.
Ik ben mij ervan bewust dat ik het woord «middelen» in de mond heb genomen, maar misschien kunnen we elkaar halverwege ontmoeten. Ik heb zojuist eigenlijk ook de diverse sectoren opgeroepen om daar zelf de schouders onder te zetten, om zelf patchbrigades rond te sturen. Dat is wat anders dan patchpolitie, maar het zou wel helpen als de Minister allerlei kwetsbare sectoren ertoe zou oproepen, misschien via de brancheorganisaties of de ondernemersverenigingen, om centraal patchbrigades het land in te sturen om de aangesloten bedrijven te helpen hun lekken te dichten.

Minister **Yeşilgöz-Zegerius**:
Wellicht kunnen we nog één stap verder naar het midden zetten om elkaar te vinden. Ik begrijp wel waar mevrouw Van Ginneken naar op zoek is. Dat past in ieder geval heel erg bij waar wij naar op zoek zijn. Dat is: hoe kan je daarin continu die alertheid houden? Dan doel ik ook echt op alle sectoren. Ik noemde net namelijk mooie getallen, maar dat betreft bedrijven en mensen die naar ons toe komen, inloggen en zeggen dat ze hulp nodig hebben. Volgens mij is mevrouw Van Ginneken ook op zoek naar hoe we degenen kunnen bereiken die daar nog niet tussen zitten of die nog niet weten dat ze ook bereikt moeten worden, terwijl ze ook een risico lopen. Daar wordt heel veel aandacht aan besteed. Ik weet niet of we met de patchbrigade helemaal het doel bereiken, al klinkt het eigenlijk wel mooi, maar we communiceren daar wel over en hebben daar aandacht voor. Daarin trek ik ook echt nauw samen op met de collega van EZK. We vragen hier continu aandacht voor, want ik denk dat mevrouw Van Ginneken gelijk heeft als ze stelt: dit zijn de mensen die naar je toe komen, maar hoe bereik je degenen die je nog moet bereiken? Dat is echt een belangrijke opdracht, die ik ook samen met EZK blijf vervullen.
Mag ik naar het mapje encryptie?

De **voorzitter**:
Zo te zien wel.

Minister **Yeşilgöz-Zegerius**:
Ik wilde het alleen even checken.
Dat is een belangrijke. Ik heb de vragen een beetje door elkaar. Ik doe ze gewoon op de volgorde die ik voor me heb. Het komt in de kern allemaal op hetzelfde vraagstuk neer.
De eerste vraag die ik hier heb, is van mevrouw Van Ginneken. Zij vroeg: wat betekent de grondwetswijziging van afgelopen woensdag over de onaantastbaarheid van digitale communicatie voor het beleid van de Minister? Volgens mij gaat dat over de aanpassing van het briefgeheim. Dat voorstel is dat iedereen recht heeft op eerbiediging van zijn brief- en telecommunicatiegeheim. Daar komt wel bij dat dit recht, zoals elk recht,

niet absoluut is. Geen enkel recht is absoluut. In lid 2 van het voorstel staat dat beperkingen van dit recht bij wet worden bepaald, met een machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Dat is juridische tekst en taal, maar dat komt erop neer dat er in die zin geen sprake is van die onaantastbaarheid van digitale communicatie. De inventarisatie die ik uitvoer over versleuteling en end-to-endencryptie ziet op de mogelijkheden om rechtmatige toegang tot versleutelde data te verkrijgen, om geïnformeerde besluitvorming mogelijk te maken en, indien een proportionele oplossing zich voordoet bij deze besluitvorming, geldende wetgeving daarin mee te nemen. Ik kan me voorstellen dat er al vragen zijn, maar misschien is het goed dat ik nog even doorga, want deze vragen liggen allemaal in elkaars verlengde. Het is ook een ingewikkeld onderwerp, waarbij het er in de basis eigenlijk op neerkomt dat we dingen aan het onderzoeken zijn. Volgens mij willen we namelijk allemaal hetzelfde. We willen aan de ene kant beschermen wat er is opgebouwd. Daarvoor is het ook nodig, end-to-end. Tegelijkertijd wil je weten of er nog extra elementen nodig zijn voor de veiligheid. Ik heb hier als Kamerlid ook moties over ingediend. Die waren eigenlijk helemaal in lijn met alle verschillende input hier.

Mevrouw Van Ginneken had namelijk ook nog de vraag: kan de Minister toezeggen de Europese Commissie aan te sporen om in de Europese inventarisatie over toegangsmogelijkheden het versleuteld bewijs en het recht op onaantastbaarheid van digitale communicatie mee te nemen? Ik heb zojuist toegelicht dat er geen sprake is van onaantastbaarheid. Dat niet. Indien de wijziging van de Grondwet wordt aangenomen, is het mogelijk om bij wet beperkingen van dit recht mogelijk te maken, zoals ik net zei: met machtiging van de rechter. Dat was die hele juridische tekst. Voor geïnformeerde besluitvorming te zijner tijd denk ik dat het goed is om verschillende mogelijkheden te beoordelen. Om deze reden is het belangrijk dat we de inventarisatie van de voor- en nadelen van rechtmatige toegang tot bewijs niet beperken. Er wordt dus nu een onderzoek gedaan in Europa. Wij doen hier in Nederland ook onderzoek. Je hebt end-to-endencryptie. We kijken daarbij wat de voor- en nadelen ervan zijn als je daar rechtmatige toegang op zou willen organiseren. Ik denk dat ik inmiddels niet de voor- en nadelen ervan ken, maar wel de voors en tegens. Ik weet dat er partijen zijn die zeggen: daar moet je gewoon niet aankomen. Er zijn ook partijen die zeggen: dat moet je wel inbouwen, want dat kan nuttig zijn. Juist omdat het zo complex is, hebben we gezegd: we gaan dit onderzoeken; we maken pas op de plaats. Dat is ook een duidelijke wens van de Kamer. Dat is ook precies hoe het vorige kabinet en dit kabinet het hebben ingericht. Bij de beoordeling straks worden al deze zwaarwegende belangen ook gewoon meegenomen, vandaar dat ik er nu heel veel woorden voor nodig heb. Ik wil mij aan geen enkele kant vastzetten, omdat we er pas met elkaar naar kunnen kijken als alles op tafel ligt, waaronder de feiten. Als het nodig is, kunnen we er daarna ook nog politiek van maken, maar laten we eerst maar eens kijken wat uit die onderzoeken komt. Ook moeten we kijken naar de geldende wet- en regelgeving. Dat spreekt voor zich.

Volgens mij was er ook nog gevraagd of de vragen van de VVD en D66 beantwoord konden worden. Ik meen dat die gisteren zijn beantwoord. Die antwoorden heeft u dus al binnen of komen nog binnen. Excuus van mijn kant dat dat niet veel eerder is gebeurd. Ik hoor dat u ze gezien heeft. Ze zijn in ieder geval gisteren verzonden.

Dan had ik nog een vraag die vooral van het CDA en de PvdA kwam, over de belangenafweging tussen fundamentele rechten. Ik noem opsporing en cybersecurity, en het wel of niet bestaan van een tegenstelling tussen privacy en veiligheid. Ik heb dit inderdaad in een van onze eerste kennismakingen – ik heb nog niet met iedereen in dit verband kennis kunnen maken, maar wel met mevrouw Kathmann – aangegeven dat ik

dat een hele ouderwetse houding vind, alsof privacy en veiligheid tegenover elkaar zouden staan. Daar geloof ik gewoon niet in. Dat is niet zo. Feit is wel dat we binnen alle waarborgen die we hebben, zien dat criminelen daar misbruik van maken. Dus hoe kun je zaken nou zo optuigen dat je niet met je handen op de rug staat en ook de goeden onder ons niet te veel belast met alles wat je vervolgens vanuit de veiligheidshoek zou willen doen? Ik denk dat dat een terugkerend thema wordt in heel veel commissies en heel veel debatten, ook in deze commissie en ook in dit verband. We zullen die onderzoeken straks zien. Daar kan ik nu nog allerlei filosofische dingen over zeggen, maar daar heeft u niks aan. Dan gebruik ik alleen maar meer woorden voor: we gaan straks kijken wat dit allemaal oplevert.
Maar uiteindelijk willen we wel echt kunnen optreden, of dat nou tegen de hackers is, de georganiseerde misdaad, de georganiseerde criminaliteit of de terroristen. Dan zul je ook bereid moeten zijn om op dat gebied stappen te zetten. Dat betekent ook dat je ruimte gaat inbouwen. Nu heb ik het niet meer specifiek over end-to-end, maar veel breder over veiligheid. We gaan namelijk zien wat er uit het onderzoek naar end-to-end komt. Je moet ruimte gaan inbouwen voor onze veiligheidsdiensten en voor de inlichtingendiensten om die criminelen voor te zijn. Als je die ruimte niet inbouwt, dan ga je ze nooit voor kunnen zijn. Zo simpel is het.
Dat betekent dat er af en toe politiek ingewikkelde afwegingen zijn, maar ik geloof wel dat we die moeten nemen en moeten maken en dat we het debat aan moeten gaan. Als privacy tegenover veiligheid blijft staan en we doen alsof dat tegengestelde belangen zijn, dan doen we onszelf namelijk behoorlijk tekort. Dan gunnen we degenen die ons kwaad willen doen wel heel veel extra ruimte. Daar ben ik echt van overtuigd. Dat zie je nu ook echt gebeuren. Dat is ook de reden waarom ik de komende tijd een aantal keren met wetgeving, grondslagen, dat soort elementen naar uw Kamer terug zal komen. Het is terecht dat u dan vraagt: waarom is dit echt nodig? Maar als we dat duidelijk kunnen laten zien – anders moeten we ook niet naar de Kamer komen – dan hoop ik daarvoor wel ruimte te krijgen. Hetgeen tegenover ons staat, is namelijk niet fictief.
Dan ben ik bij het blokje overig.

De **voorzitter**:
Mag ik nog één aanvullende vraag stellen? Ik zie mevrouw Kathmann ook nog. Kan het zijn dat naarmate dit onderzoek vordert ... We hebben natuurlijk ook kwantumcomputers die inmiddels al daar zijn, albeit niet overal. Kan dat nog van invloed zijn op de keuze of, nou ja, op de discussie?

Minister **Yeşilgöz-Zegerius**:
Dat hangt ook een beetje van de snelheid van die ontwikkelingen af en van dat soort elementen, maar daar wordt absoluut naar gekeken. Mevrouw Van Weerdenburg heeft daar natuurlijk helemaal gelijk in. Terwijl je iets aan het onderzoeken bent en afwegingen op tafel aan het brengen bent met betrekking tot de voor- en nadelen, word je ingehaald door technologische ontwikkelingen. Dat is ook wat dit vakgebied zo leuk en spannend maakt. Dus op het moment dat dat echt moet worden meegewogen, dan nemen we het mee. Ik kan niet beloven dat dat al volledig in het onderzoek van de Commissie meegenomen is, maar dat is dan wel iets voor ons om hier ook weer op tafel te leggen.

Mevrouw **Kathmann** (PvdA):
Mijn diepe reflectie ging eigenlijk ook over het volgende. Juist op het moment dat de Minister komt met een vraag om meer toegang of een wettelijke grondslag, zodat er in het kader van de veiligheid meer mogelijk is, dan mis ik vaak de discussie hoe het zit met de waarborgen die daarbij

horen. We bespreken vaak het stuk: we hebben gewoon in het kader van de veiligheid die juridische grondslag nodig. En dan bespreken we los het stuk: met de toezichthouders en de waarborgen van die grondslag zit het zo. Ik zou zo graag willen – anders doen we onszelf tekort – dat we dat in één pakket doen. Anders blijven we steeds als er een nieuwe wettelijke grondslag voorbijkomt in deze commissie maar hangen in «degene die de wettelijke grondslag geen groen vinkje wil geven, is tegen veiligheid» en «degene die dat wel wil doen, heeft lak aan de privacy». Daarom is het ook zo'n integraal vraagstuk. Dat mis ik. Ik hoop dus dat we een manier kunnen vinden dat we, als de Minister komt met een vraag voor een wettelijke grondslag, in één brok het hele bakje van waarborgen waarin het valt, kunnen bespreken.

Minister **Yeşilgöz-Zegerius**:
Dat deel ik wel. Daar zal ik dus vanuit mijn rol mijn best voor doen. Daar heb ik wel de hulp van de Kamer bij nodig, ook om de debatten vervolgens op die manier te kunnen voeren. Nu nemen ik en mevrouw Kathmann allebei een voorschot op wat wel of niet gaat komen, maar we weten volgens mij allebei vanuit het verleden waarom het wel goed is als we het gesprek op tijd hebben en niet op het moment dat het allemaal al op tafel ligt. Vanuit mijn rol zal ik dat dus zeker inbrengen. Maar help me, of het nou iemand is die zegt «ik vind het heel goed dat dit gebeurt» of «dit gaat gewoon te ver». Waarom doen we dit? Waarom ligt het op tafel? Wat is het nut? Wat is de noodzaak? Wat is de urgentie? Dan is het aan ons om dat goed te verwoorden. Hoe kan het dan wel goed vanuit die urgentie? Dat is primair ons werk. We zijn heel druk bezig met alle elementen die gaan komen binnen die waarborgen. Maar mocht het als niet genoeg of als te weinig worden ervaren, denk dan ook met ons mee. Dat is namelijk waar je anders in terechtkomt. Dan is het namelijk heel erg polariserend tegenover elkaar. Dan is het gewoon een ja of een nee. Dan komt het er eigenlijk op neer dat wij heel erg met elkaar bezig zijn en dat degenen tegenover wie we staan, voor wie die wetgeving nodig is, gewoon zijn goddelijke gang kan gaan. Dat is de frustratie die ik ook deel. Vanuit mijn rol zal ik daar dus mijn best voor doen, maar ik weet nu al dat ik de Kamer daarbij nodig ga hebben, van welke partij men dan ook komt of aan welke kant men dan ook staat. Het liefst is er natuurlijk geen kant, maar doen we het gewoon samen. Maar dat heb ik wel nodig.

De **voorzitter**:
Helder. Bent u al toe aan het blokje overig?

Minister **Yeşilgöz-Zegerius**:
Zeker. Daar ben ik. Mevrouw Rajkowksi had een vraag over de ABDO. Zij had het over een plan voor de Algemene Beveiligingseisen voor Defensie-opdrachten, voor de gehele rijksoverheid. Het is goed om te zeggen dat mevrouw Rajkowski vier belangrijke punten had waarvan ze zei: ik zou het mooi vinden als ze in de strategie landen. Ik ga die afzonderlijk benoemen en behandelen. Zoals ik aan het begin van mijn betoog al zei, past het naadloos bij hoe er naar de strategie wordt gekeken door mijn departement en door alle collega's. Die zullen daar dus in landen. Ik zal daar nu kort op ingaan, maar die zullen er allemaal in terugkomen.
Veilige inkoop en aanbesteding heeft uiteraard de volle aandacht van het kabinet. Ten aanzien van de nationale veiligheidsrisico's geldt daarom dat eind 2018 verscherpt inkoop- en aanbestedingsbeleid geldt. Daarbij is opgenomen dat bij inkoop en aanbesteding mogelijke risico's voor de nationale veiligheid per inkoopopdracht worden meegenomen. Daarbij is een instrument ontwikkeld waarmee informatiebeveiligingseisen rond ICT-aankoop en -aanbestedingen geformuleerd kunnen worden ten behoeve van het contract. Een regeling voor de gehele rijksoverheid, analoog aan de ABDO, kan helpen deze inzet op veilige inkoop verder te

versterken. Dit zal ik ook opnemen met mijn collega van BZK. Wij zullen dat onderzoeken en daarop komen we terug in het najaar.
Mevrouw Van Ginneken vroeg: waarom is het nationaal coördinatiecentrum voor cybersecurity, kennis en innovatie van het Ministerie van EZK niet ondergebracht bij NCSC of het Digital Trust Center? Het nationaal coördinatiecentrum voor cybersecurity, kennis en innovatie is onderdeel van het Europese netwerk van zogenaamde Cybersecurity Competence Centres. Het coördinatiecentrum gaat onder meer Europese onderzoekfondsen, zoals Digital Europe, in Nederland verdelen. Bij deze fondsen kunnen bedrijven en overheidsorganisaties onderzoeksvoorstellen indienen voor subsidie. En om deze reden, dus om belangenverstrengeling te voorkomen, is het van belang dat het centrum zelfstandig van andere partijen wordt gepositioneerd. Dat heeft dus een heel feitelijke reden: we willen geen belangenverstrengeling.
De PvdA heeft een vraag gesteld over de proeftuin in Roermond. Het is wellicht goed om iets over de proeftuin zelf te zeggen. Dit loopt al heel lang. Ik zei net tegen de collega's: hé, hier was ik als woordvoerder veiligheid ook al mee bezig toen ik Kamerlid was. Dit komt hier dan weer terug. In Roermond was er een samenwerkingsverband van de politie, het Openbaar Ministerie en de gemeente. De focus lag op het tegengaan van mobiel banditisme in de vorm van winkeldiefstal en zakkenrollerij in het winkelgebied van de Designer Outlet Roermond. De politie maakte daarbij gebruik van een netwerk van ANPR-camera's met een achterliggend algoritme, op basis van kenmerken van de in het lokaal veiligheidsbeeld beschreven werkwijze van de internationale dadergroep die in Roermond verantwoordelijk was voor mobiel banditisme. Als een voertuig dat langs de ANPR-camera's reed in voldoende mate voldeed aan de kenmerken van de dadergroep, was er sprake van een hit, waarna opvolging door een politie-eenheid ter plaatste volgde. De politie gebruikte daar als kenmerken onder meer bepaalde merken of typen auto's. Daarbij ging het met name over Duitse merken. De nationaliteit van het kenteken was ook een kenmerk, namelijk Roemeens, Bulgaars of Brits. Ook werd gelet op de gereden route, bijvoorbeeld vanaf de grens richting de Designer Outlet.
In de Kamerbrief die nu op de agenda staat, geeft mijn ambtsvoorganger aan dat de aanpak die in de proeftuin is gehanteerd, in principe binnen de grenzen van de wet valt. Maar de proeftuin is inmiddels wel gestopt. De proeftuin kwam in 2020 stil te liggen omdat er onvoldoende politiecapaciteit was om de hits op te volgen, én omdat vanwege de coronamaatregelen het criminaliteitsbeeld veranderde. Daarmee verdween het doel van de gegevensverwerking. En als je niets met de verzamelde gegevens gaat doen en je dat vooraf al weet, is de verwerking niet proportioneel en mag je de gegevens dus gewoon niet meer verzamelen. De verzamelde gegevens zijn dan ook direct verwijderd toen de proeftuin stil kwam te liggen.
Hoewel de proeftuin door het gebrek aan opvolgcapaciteit en door het veranderde criminaliteitsbeeld maar zeer beperkt tot uitvoering is gebracht, is de operationele toegevoegde waarde niet geëvalueerd. Toch heeft de proeftuin wel heel veel kennis opgeleverd over de technische mogelijkheden van sensortechnologie, over de juridische mogelijkheden en onmogelijkheden, en over ethische vraagstukken die met het gebruik van sensortechnologie worden geadresseerd. Zo wordt over ethische vraagstukken bijvoorbeeld meegenomen dat het goed is om bij dergelijke projecten voorafgaand een ethische toets uit te laten voeren. Dus de proeftuin is gestopt vanwege de net genoemde redenen, en we hebben er ook nog lessen voor de toekomst van geleerd. Als je zoiets weer zou willen doen, moet je bijvoorbeeld vooraf zo'n toets doen. Wat mij betreft moet je er ook vooraf op die manier goed over communiceren, zodat je niet achteraf op die manier een discussie krijgt.

Mevrouw **Kathmann** (PvdA):
Mijn vraag was eigenlijk of alle soortgelijke proeftuinen zijn gestopt. Want dat deze proeftuin in Roermond gestopt is, was inderdaad duidelijk. Ik vroeg ook om een soort concrete lijst met waarborgen die je stelt voordat je zo'n proeftuin inricht. Ik ben heel blij met het voorschot van de Minister in haar antwoord, over die toets vooraf. Maar mijn vraag is dus concreet: kan er een lijst opgeleverd worden met concrete waarborgen, waarborgen waaraan moet worden voldaan voordat zo'n proeftuin wordt ingericht? En ik wil dat alle proeftuinen worden gestopt totdat er zo'n lijst met waarborgen is.

Minister **Yeşilgöz-Zegerius**:
Ik heb er geen beeld van welke proeftuinen er op dit moment allemaal zouden zijn. Maar zoals gezegd: het standpunt hierbij is wel dat het binnen de kaders van de wet moet vallen als je zo'n proeftuin begint, en dat wat je daarna ophaalt ook proportioneel is. De grenzen van de wet die ons zijn meegegeven, zijn je waarborgen. En zodra er niet voldoende politiecapaciteit is om het op te volgen, is het meteen al niet meer proportioneel. Want dan verzamel je gegevens om het verzamelen en dat kan niet. Dus ik denk dat die waarborgen er juist wel zijn. Het feit dat we er direct mee zijn gestopt toen we er niet meer aan voldeden, laat dat ook zien. Maar die toetsen worden altijd vooraf gedaan. En als mevrouw Kathmann dat waardeert, kan ik natuurlijk wel op papier zetten wat dan zo'n afweging is. Wat zijn de proportionaliteitsafwegingen en welke andere elementen worden daarin allemaal meegewogen? Maar die zijn er, want dat is de wet. Wij moeten ons aan de wet houden. En «wij» bedoel ik hier heel breed; ik speek nu namens de politie.

Mevrouw **Kathmann** (PvdA):
Volgens mij zijn dat ethische vraagstuk en die toets niet van tevoren meegenomen. Want de Minister zegt: we hebben er nou juist van geleerd en dat gaan we vanaf nu doen. Ook bij de waarborgen die ik bedoel, hoort zo'n ethische toets. De Minister is van mening dat er binnen de wet is geopereerd. De Partij van de Arbeid is dat helemaal niet van mening. Er wordt gesuggereerd dat er alleen maar aan ANPR-technologie wordt gedaan, maar er wordt gewoon aan profilering gedaan. Er worden profielen opgebouwd. Die profielen worden een jaar bewaard. Dat is heel iets anders dan ANPR, waarmee je een nummerbord leest op het moment dat er iets aan de hand is en je echt op zoek bent naar een specifieke dader. Dat zijn heel verschillende dingen. Ik vond de manier van corresponderen over Amnesty International ook echt gebrekkig en van een heel laag niveau, maar ik denk dat dit misschien niet het moment is om daarover te discussiëren. Ik stel mijn vraag dus nogmaals. Ik wil weten bij welke proeftuinen die nog lopen die ethische toets nog niet is gedaan. Kan er ook een lijst komen met waarborgen, zodat we erop kunnen rekenen dat, als er ooit nog proeftuinen worden ingericht, dat in ieder geval binnen de wet gebeurt?

Minister **Yeşilgöz-Zegerius**:
We kunnen van mening verschillen. Dat staat eenieder vrij. Maar ik ga niet mee in het frame dat het niet binnen de wet is geweest. Daarover heb ik een heel duidelijk standpunt. Ik zei wel – dat ben ik volledig met mevrouw Kathmann eens – dat je aan de voorkant goed moet communiceren. Dat is een van de elementen die de politie actief heeft opgepakt en heeft geleerd. Dat past wel in waar mevrouw Kathmann denk ik naar op zoek is: je moet vooraf laten zien welke afwegingen er zijn gemaakt en welke kaders er zijn gevolgd om aan zoiets te beginnen. Dat zijn juridische en ethische afwegingen. De politie is, ook als het gaat over de inzet van sensortechnologie, heel kritisch aan het bekijken hoe je kunt laten zien met welke afwegingen je dat doet. Natuurlijk zal ik bij de politie opvragen

of ze daar nu al iets over kunnen melden. Ik zal daar dus op terugkomen. Als dat al kan, stuur ik dat toe. Ik zal die brief sowieso sturen. Als de kaders en de formulering vooraf nog in ontwikkeling zijn, laat ik dat ook weten. Als een en ander er al is, deel ik dat. Ik wil er nog wel bij zeggen dat ik niet uitsluit dat er in proeftuinen of whatever instrumenten worden gebruikt om achter grootschalige criminele activiteiten te komen en daar proactief op te kunnen acteren waarvan we wellicht nog steeds van inzicht verschillen over of dat wenselijk is of niet. Maar zolang het binnen de wet gebeurt en er vanwege de veiligheid wordt aangegeven dat het nodig is, zal ik daarvoor staan. Daarover kunnen we politiek dus wellicht van mening verschillen. Maar ik ben het met mevrouw Kathmann eens dat je aan de voorkant moet weten wat de kaders zijn. Die zijn volgens mij helder. Ze worden nog meer verhelderd door de politie, omdat ze zelf ook zagen dat je dat aan de voorkant beter moet communiceren. Ik kom dus met een brief. Ik heb nu al iets meer toelichting gegeven over wat er wel en niet in kan staan, maar ik hoop dat mevrouw Kathmann begrijpt dat ik even moet ophalen wat er allemaal wel of niet over is uitgezocht. Maar ik begrijp waar zij naar op zoek is, dus daar gaan wij achteraan.

De **voorzitter**:
Dank u wel. Daarbij wil ik ook opmerken dat we met de collega's ervoor moeten waken dat we niet al te veel op het terrein van de vaste commissie voor Justitie komen, want niet iedereen hier aanwezig is tevens woordvoerder op dat onderwerp. We kunnen door naar het volgende punt.

Minister **Yeşilgöz-Zegerius**:
Ja, helder, voorzitter. Ik zal ervoor zorgen dat ik in de brief met name inga op de pilot en de sensortechnologie, want dat ligt wel heel erg hier. Ik denk dat dat het dichtste komt bij waar mevrouw Kathmann nu naar op zoek is. Als er andere elementen zijn, kan die brief ook in de andere commissie geagendeerd worden. Dan doen we dat zo.
Er is nog gevraagd naar de bewustwording bij consumenten over slimme apparaten. Hartstikke mooi dat ik de heer Bontenbal in een andere commissie toch weer tegenkom. Hij stelt mooie vragen, die óók bij Economische Zaken en Klimaat thuishoren: híér en dáár. Over de bewustwording bij consumenten voert de Minister van EZK de publiekscampagne «Doe je updates» uit. Terwijl ik dit uitspreek, denk ik: dat zou ik thuis ook moeten doen. Daar ga ik dus ook mee aan de slag. Daarnaast kunnen burgers voor informatie en advies altijd terecht op veiliginternetten.nl. Die website heeft jaarlijks circa 1 miljoen unieke bezoekers, dus er is geloof ik wel heel veel behoefte aan om daarop te bekijken wat je kunt doen. Ik denk dat het goed is als wij daar in al onze verschillende rollen aandacht aan blijven besteden, voor alle kijkers thuis. Dat doet mijn collega van EZK dus ook.
Ik heb nog twee vragen liggen. De heer Bontenbal vroeg wat de concrete doelen van de Roadmap Digitaal Veilige Hard- en Software zijn en hoe die wordt geëvalueerd. Het doel is om het algehele niveau van de cybersecurity van ICT-producten en -diensten en het internet of things te verhogen. Het is een complex en grensoverschrijdend vraagstuk waarvoor een mix aan maatregelen nodig is, variërend van bewustwording van gebruikers tot certificering en wettelijke maatregelen in de EU. Die roadmap wordt momenteel geëvalueerd door een extern onderzoeksbureau. U zult dit rapport voor de zomer ontvangen. De resultaten worden door de Minister van Economische Zaken en Klimaat meegenomen in de nieuwe Nederlandse cybersecuritystrategie, die we uiteraard gezamenlijk opstellen. Dus dat komt voor de zomer.
Dan heb ik als laatste de vraag van mevrouw Van Weerdenburg over de Kwetsbaarheden Analyse Tool. Het gaat over een brief van VWS. Die is gerealiseerd in tijden van de coronacrisis. Dat lijkt onwijs lang geleden,

maar dat valt wel mee. Toen is de noodzaak hoog gebleken om snel en betrouwbaar voor de bestrijding van de pandemie ontwikkelde digitale hulpmiddelen op het juiste beveiligingsniveau te kunnen brengen en te houden. Dat gaat bijvoorbeeld over de voortdurende monitoring van het CoronaCheck-stelsel.
Voorzitter. Die Kwetsbaarheden Analyse Tool wordt op dit moment specifiek toegepast op het zorgdomein, zoals mevrouw Van Weerdenburg al aangaf. We delen dit soort best practices ook. Volgens mij vroeg mevrouw Van Weerdenburg concreet of andere collega's of instellingen dit ook doen. Dus je deelt dit soort best practices met de collega's, met andere departementen, met andere sectoren om te kijken of er elementen in zitten die ook specifiek voor jou van toepassing zijn. Op die manier wordt dat in die zin breder opgepakt of uitgezet.

De **voorzitter**:
Dank voor dat antwoord. Ik begreep uit de brief dat er een aanbod was om de Tweede Kamer te scannen met die tool, dat dit ook daadwerkelijk gebeurd is en dat daar gelukkig niks gruwelijks uit kwam. Mijn vraag was: zijn er ook ministeries gescand? Ik geloof dat het ook de bedoeling was dat die tool in de eerste helft van dit jaar als open source beschikbaar zou komen. Ik denk dat het daarmee dan ook voor andere ministeries beschikbaar is. Ik vroeg me meer af of er een bepaalde taskforce of een initiatief of wat dan ook is om de rest van de ministeries ook te scannen.

Minister **Yeşilgöz-Zegerius**:
Ik kom er zo in tweede termijn even op terug. Dan weet ik of ik er nog iets explicieters over kan zeggen.

De **voorzitter**:
Dank. Dan kijk ik even naar de overige leden. Mevrouw Rajkowski heeft nog een vraag.

Mevrouw **Rajkowski** (VVD):
Ik mis nog – of ik heb 'm gemist – punt drie van de vier punten, over de ISIDOOR-oefeningen.

Minister **Yeşilgöz-Zegerius**:
Ja, die heb ik. Dat is waar. Daar heeft mevrouw Rajkowski helemaal gelijk in. Ze vroeg: oefenen is heel goed, dus kan dat niet vaker?

Mevrouw **Rajkowski** (VVD):
En integraal.

Minister **Yeşilgöz-Zegerius**:
Ja, integraal en vaker. Ik ben het in essentie eens dat vaker ook goed zou zijn. Er zitten wel twee kanttekeningen bij, waardoor je niet zomaar «ja, dat gaan we doen» kunt zeggen. Ten eerste heeft het te maken met capaciteit. Je moet ook zorgen dat je het waar kunt maken. Vanuit de experts werd ook benadrukt dat je tijd nodig hebt om te leren van zo'n oefening. Dus dat vraagt ook tijd. In essentie geldt dus dat als het vaker kan en moet, je dat ook moet doen. Daar hebben we dus vol aandacht voor. Maar dat is om deze twee redenen niet altijd opportuun of mogelijk. Integraal, cross-sectoraal, is sowieso waar we naartoe bewegen. In de volgende oefening zal daar ook meer aandacht voor zijn. Dat moet je op die manier ook steeds meer uitbouwen. Ook dit element komt weer terug in de strategie.

Mevrouw **Rajkowski** (VVD):
Heb ik 'm dan zo goed gehoord? Die ISIDOOR-oefeningen zijn natuurlijk supergoed. Heel veel organisaties doen mee. Maar die oefeningen zijn zo

gericht op de digitale wereld, dat ik denk: zo werkt het natuurlijk eigenlijk niet. Hoor ik hier dan de toezegging dat een volgende ISIDOOR-oefening veel meer die verbondenheid en verwevenheid met de fysieke wereld heeft?

Minister **Yeşilgöz-Zegerius**:
Ja, daar wordt steeds meer die samenhang in gezocht, precies om de reden die mevrouw Rajkowski aangeeft: het is al zo breed dus in één keer zeggen «het is echt volledig integraal en het sluit volledig op elkaar aan» is een te grote stap. Maar daar wordt steeds meer die samenhang in gezocht, omdat de meerwaarde daarvan absoluut wordt gezien.

De **voorzitter**:
Tot slot, mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Nog een kleine aanvulling dan. Wij krijgen altijd informatie als een ISIDOOR-oefening is geweest, vaak wat op hoofdlijnen. Dat begrijp ik ook. Zou daar ook kunnen worden ingegaan op wat er nieuw was of wat er geoefend is?

Minister **Yeşilgöz-Zegerius**:
Yes.

De **voorzitter**:
Dank u wel. Dan kijk ik even naar links om te zien of er behoefte is aan een tweede termijn. Ik zie: nee, nee en ja. Oké, dan doen we een korte tweede termijn. Zullen we even pauze houden?

Minister **Yeşilgöz-Zegerius**:
Ja graag, want ik heb een aantal dingen naar de tweede termijn doorverwezen. Als ik een paar minuten krijg, dan kan ik de antwoorden even bekijken en zo gericht mogelijk reageren.

De **voorzitter**:
Dan schors ik de vergadering vijf minuten.

De vergadering wordt van 15.44 uur tot 15.48 uur geschorst.

De **voorzitter**:
Aan de orde is de tweede termijn. Ik geef het woord aan mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Dank ook voor de uitgebreide beantwoording. Ik denk dat de conclusie van de beantwoording van de Minister een beetje is dat wij de cybersecuritystrategie allemaal heel goed gaan lezen. Ik denk ook dat we daar heel veel zin in hebben, als ik kijk naar wat voor mooie punten daar allemaal in gaan komen.
Ik wilde ook nog even een soort side note maken. Ik vond het ook mooi om aan het begin te horen dat verschillende ministeries achter de schermen aan het samenwerken zijn om deze vragen te beantwoorden. Zo gaan we het varkentje van de cybersecurity volgens mij wel wassen. Complimenten ervoor dat er achter de schermen wordt samengewerkt. Dank ook ervoor dat die vier punten gaan terugkomen, met name het punt over de hackers die op de sanctielijsten komen te staan. Daar kijken wij reikhalzend naar uit.
Ik had nog één zorg. Die gaat over het sneller en specifieker delen van dreigingsinformatie door het DTC. Volgens mij omarmen we allemaal dat dat belangrijk is, maar ik zou toch nog iets meer comfort willen krijgen

van de Minister in die zin dat zij zegt dat dit belangrijk is en dat daar snel oplossingen voor moeten komen naar de Kamer. Misschien kunnen we daarover extra geïnformeerd worden. Graag een reactie van de Minister.

De **voorzitter**:
Dank u wel. Het woord is aan mevrouw Van Ginneken.

Mevrouw **Van Ginneken** (D66):
Dank, voorzitter in de eerste plaats. In de tweede plaats dank aan de Minister voor de uitgebreide beantwoording. Het is fijn dat we met ruimhartige interrupties tot een goed gesprek zijn gekomen. Net als collega Rajkowski kijk ik ook naar de nu al enigmatische nieuwe cyberstrategie die de Minister voor de zomer naar ons toe gaat sturen. Ik ben erg benieuwd welke oplossingen er komen. Ik ben blij dat we dezelfde kant opkijken en dat we versnippering terugdringen.
Ik ben ook blij met de toezegging van de Minister dat daarin te lezen gaat zijn wat we wel en wat we niet kunnen doen met de beschikbare middelen. Dan kunnen we daar een goed gesprek over voeren met elkaar.
Ik wil nog even twee punten aanstippen. Ten eerste encryptie. De Minister heeft aangegeven dat de onaantastbaarheid van de vertrouwelijkheid niet absoluut is. Dat is natuurlijk zo. Ik ben blij om te horen dat de Minister proportionaliteit als belangrijk criterium daaraan koppelt. D66 kan zich niet voorstellen hoe een generieke achterdeur proportioneel is, maar ik wacht de resultaten van het onderzoek van de Minister af.
Tot slot, voorzitter. We hebben gesproken over de vraag of we niet meer moeten doen om bedrijven weerbaarder te maken tegen de sowieso toenemende dreiging en de eventueel aanvullende dreiging vanwege de situatie in Oekraïne en de rol van Rusland. Ik ben niet helemaal tevreden met het antwoord van de Minister, want zij zegt: we organiseren webinars, we bereiken de mensen die toch al ontvankelijk zijn. Ook ben ik niet helemaal tevreden over de reactie van de Minister op mijn oproep tot het stimuleren van patchbrigades. Ik ga ook nog even kijken naar de antwoorden die de Minister heeft gegeven op de schriftelijke vragen over encryptie. Dat vergat ik nog te zeggen. Vanwege die twee losse eindjes zou ik heel graag een tweeminutendebat willen aanvragen.

De **voorzitter**:
Dank u wel. De Minister kan gelijk antwoorden in tweede termijn.

Minister **Yeşilgöz-Zegerius**:
Veel dank. Veel dank ook voor de aankondiging van wat ik kan verwachten in het tweeminutendebat, maar ook voor de woorden. Wellicht ga ik maar even meteen concreet in op de vragen die ik nog had staan en de nieuwe vragen. Ik heb het helemaal eens met mevrouw Rajkowski. Wij moeten snel kunnen handelen vanuit de diensten die wij hebben, zoals DTC. Het is gewoon ontzettend belangrijk om ervoor te zorgen dat de informatie op de juiste manier belandt waar die moet belanden. Wij zullen daar absoluut alle aandacht aan besteden en er alles aan doen om dat goed op orde te krijgen. Als dat wenselijk of nodig is, kunnen we daar bijvoorbeeld ook technische briefings over organiseren. Wij kunnen daarover dus ook wel meer aanbieden. Dat zijn dus twee zaken. Er is altijd meer informatie mogelijk. Dat kan via een technische briefing. Daar kan de Kamer altijd om verzoeken. Bovendien zullen wij in als ons werk alles op alles zetten om dat goed te regelen. Dat was die vraag.
Dan ga ik het rijtje af van de vragen die ik nog binnen heb gekregen en de vragen die nog openstonden. De heer Bontenbal vroeg wat voor soort bedrijven bij DTC zijn aangesloten op de informatiediensten over de kwetsbaarheden en de digitale dreigingen. Er doen grote en kleine bedrijven mee aan de pilot over het notificeren van het Digital Trust Center en het Nationaal Cyber Security Centrum. Zij komen uit negen

sectoren, zoals bouw, transport en media. Het is dus erg divers. Over de bedrijven die ongevraagd zijn geïnformeerd door het DTC, is op dit moment geen informatie voorhanden. De Minister van EZK zal uw Kamer voor de zomer een brief sturen over dit onderwerp. Daar zal ook de voortgang van de informatiedienst van het DTC in staan, dus er komt ook daarover meer informatie aan.
Volgens mij had mevrouw Rajkowski nog een vraag of mkb-bedrijven ook verplichtingen krijgen met betrekking tot cybersecurity als er sprake is van een maatschappelijk risico, bijvoorbeeld in de haven. Dat was een specifiek voorbeeld binnen de vraag naar mainports en de keurmerken, geloof ik. Op dit moment gelden inderdaad wettelijke verplichtingen voor bedrijven die aangewezen zijn als aanbieder van een essentiële dienst onder de Wet beveiliging netwerk- en informatiesystemen. Zoals ik al eerder aangaf, worden deze verplichtingen de komende jaren uitgebreid naar een groter aantal bedrijven en sectoren. We zullen bij de implementatie goed moeten blijven kijken of alle bedrijven waarvoor dit op basis van risicobeoordelingen noodzakelijk is, binnen de reikwijdte van deze wet vallen. We willen natuurlijk dat alle bedrijven die hieronder moeten vallen, eronder vallen, maar je moet het ook verder waar kunnen maken en het moet ook logisch zijn dat een bedrijf eronder valt. Daar is dus ook alle aandacht voor.
Ik was nog een antwoord verschuldigd ...

Mevrouw **Rajkowski** (VVD):
Dat klinkt heel compleet. Dat is inderdaad onder andere de Europese NIS 2-richtlijn, die ook in Nederland gaat gelden. Alleen duurt het nog even voordat al die regels ook in Nederland gaan gelden. Cybercriminelen gaan niet op die regels wachten, dus dat moeten wij eigenlijk ook niet doen. Zijn er al stappen die genomen kunnen worden? Dat kan meegenomen worden in de cybersecuritystrategie. Dat is voor mij prima, want die komt snel. Zijn er nog stappen die wij kunnen zetten, zodat wij niet wachten op wat er uit Europa komt en wij nu al weerbaarder zijn?

Minister **Yeşilgöz-Zegerius**:
We staan niet stil. Het zal niet voor alle bedrijven gelden, dus je neemt nu al stappen om te kijken hoe je nog beter kan samenwerken en hoe je kan zorgen dat je een sluitende aanpak met elkaar organiseert. Dat doen we bijvoorbeeld in de Rotterdamse haven via het project FERM, waarbij bedrijven binnen de haven samenwerken aan het verbeteren van hun cybersecurity. Dat betekent dus dat er ook hard wordt gewerkt aan het stimuleren van weerbaarheid binnen ketens, en niet alleen bij individuele bedrijven of wat je, even in mijn woorden, zou afdwingen met Europese regelgeving. Dus dat wordt zeker meegenomen ... Dat wordt al gedaan. Dat wordt niet meegenomen, maar dat wordt al gedaan. Dat kunnen we meenemen in de strategie; dat wilde ik eigenlijk nog toevoegen.

Mevrouw **Rajkowski** (VVD):
Een kleine toevoeging, want FERM is inderdaad een heel goed initiatief, maar je ziet ook dat juist degenen in de Rotterdamse haven die daarbij zijn aangesloten, vaak al best veel aandacht voor hun cybersecurity hebben. Ik vind het juist interessant om te kijken naar kleinere bedrijfjes. Maar als dit op die manier wordt meegenomen – hoe kunnen we mensen verleiden om meer bij dit soort initiatieven aan te sluiten? – dan is dat prima.

Minister **Yeşilgöz-Zegerius**:
Dan heb ik nog specifiek een aanvulling op de vraag van mevrouw Kathmann over Kaspersky: waarom niet breder nu al als je kijkt wat er om ons heen gebeurt? De afweging die we hebben gemaakt, heb ik al toegelicht. Antivirussoftware heeft vergaande systeemrechten om zijn werk te kunnen doen. Dat is de reden dat er bij misbruik een hele grote

veiligheidsdreiging is. Dat is de reden waarom je daar echt op kunt inzetten. Dat gaat over dreigingen op het gebied van spionage en dat soort elementen, dus dan heb je een gegronde reden om te zeggen: dit gaan we uitfaseren en uitsluiten; dit willen we niet. Het ding is dat besluiten als deze wel voor een rechter moeten standhouden, dus je moet het op deze manier ook kunnen onderbouwen. Als je dat niet kan onderbouwen, dan kan je dat niet doen. Ik voel wel mee met mevrouw Kathmann, eerlijk gezegd, dus we hebben net even doorgevraagd hoe dat dan werkt. Hoe zit het dan, als je met gezond verstand kijkt naar wat er om je heen gebeurt? Je kunt bedrijven of producten niet uitsluiten – sowieso niet makkelijk, gelukkig maar – ook niet op basis van wat we nu met elkaar waarnemen. Dan moet je het echt op deze manier kunnen onderbouwen. Dat kon hier specifiek wel. Breder, op het moment dat het kan, dan doe je dat, maar als het niet kan, dan kan je dat dus niet doen. Maar goed, dat dekt om die reden de lading.
Ik kom nog even terug op mevrouw Van Weerdenburg zei over de tool van VWS, zogezegd. Zij vroeg: is er een of andere taskforce of een plek ergens waar dit bij elkaar komt? De Staatssecretaris Koninkrijksrelaties en Digitalisering is stelselverantwoordelijk voor een digitaal veilige rijksoverheid. We hebben de chief information officer-Rijk, die steeds samen met departementale CIO's kijkt hoe gezocht kan worden naar risico's en hoe de weerbaarheid daarop verhoogd kan worden. Dat is een continu proces, dus daar komt het bij elkaar. Als dit iets zou kunnen zijn waarvan we zeggen «dit zijn best practices; dit kan je breder uitrollen», dan komt het daar bij elkaar. Je zou het, als je het heel graag wil, een taskforce kunnen noemen. Het is het niet helemaal, maar het gebeurt daar wel.

De **voorzitter**:
Toevallig of niet toevallig zitten wij volgende week met haar om de tafel, dus dan nemen we dat gelijk mee. Dank.

Minister **Yeşilgöz-Zegerius**:
Ik heb nog een nabrander, want ik heb iets niet goed gezegd. Dat gaat over de Wet bevordering digitale weerbaarheid bedrijven. Ik heb een aantal wetten door elkaar gehaald. Deze wet is afgelopen vrijdag naar de Raad van State verzonden, dus het is niet zo dat de raad daarover al input heeft geleverd. Dat gaat de raad nu vast doen nadat ik dit heb gezegd. Er zijn heel veel reacties uit de consultatie, waardoor het proces enigszins vertraagd is. Die twee elementen heb ik door elkaar gehaald.

De **voorzitter**:
Helder, dank u wel. Dan ga ik nu even de toezeggingen voorlezen.
– Wij hebben de toezegging dat de langverwachte – reikhalzend kijken wij ernaar uit – Nederlandse cybersecuritystrategie voor de zomer naar de Kamer zal worden verzonden. Daar zullen ook de investeringen in cybersecurity verder worden toegelicht en uitgewerkt. Ook een eventuele stelselwijziging zal dan goed uitgelegd worden. Op ons verzoek zal dat ook op schematische wijze worden weergegeven.

De term «voor de zomer» is altijd een beetje tricky. Kan de Minister iets specifieker zijn? Is dat vlak voor de zomer? Kunnen wij het nog voor de zomer bespreken?

Minister **Yeşilgöz-Zegerius**:
Uw inleiding laat zien hoe breed en hoe integraal het is, maar de planning is dat de cybersecuritystrategie begin juli in de ministerraad ligt. Ik hoop heel erg dat we dat halen. Het betekent dat de strategie net voor het reces naar uw Kamer zal komen. Mochten we het niet halen, vanwege het belang en de enorme reikwijdte ervan, dan zal ik zorgen dat ik dat netjes aankondig in de Kamer. Maar vooralsnog is dit de planning die haalbaar lijkt.

De **voorzitter**:
Oké, daar gaat u uw stinkende best voor doen. Duidelijk. Wij duimen mee. Dan is er een tweede toezegging genoteerd.

– De Minister stuurt een brief over de inzet van sensortechnologie in proeftuinen en de proportionaliteitsafwegingen en kaders die aan de start van een dergelijk project worden ingezet om de waarborgen aan de voorkant te toetsen. Dat is een toezegging aan mevrouw Kathmann.

Verder is er een tweeminutendebat aangevraagd met als eerste spreker mevrouw Van Ginneken.
Volgens mij zijn we er dan nog voor de eindtijd. Complimenten aan alle deelnemers. De kijkers thuis bedankt voor de aandacht. Graag tot een volgende keer. Ik sluit de vergadering.

Sluiting 16.01 uur.