Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 961

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 20 januari 2023

De vaste commissie voor Digitale Zaken heeft op 15 december 2022 overleg gevoerd met mevrouw Yeşilgöz-Zegerius, Minister van Justitie en Veiligheid, over:

– **de brief van de Minister van Justitie en Veiligheid d.d. 10 oktober 2022 inzake Nederlandse cybersecuritystrategie (NLCS) (Kamerstuk 26 643, nr. 925).**

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

De voorzitter van de commissie,
Kamminga

De griffier van de commissie,
Boeve

kst-26643-961
ISSN 0921 - 7371
's-Gravenhage 2023

Voorzitter: Kamminga
Griffier: Van Tilburg

Aanwezig zijn vijf leden der Kamer, te weten: Dekker-Abdulaziz, Kamminga, Koekkoek, Rajkowski en Van Weerdenburg,

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

Aanvang 10.08 uur.

De **voorzitter**:
Goedemorgen allemaal. Ik open de vergadering. Aan de orde is een commissiedebat van de commissie voor Digitale Zaken over de Nederlandse cybersecuritystrategie. We starten iets later dan dat u van ons had mogen verwachten, maar dat was omdat – het zal u niet ontgaan zijn – de weg wat glad is, dus zowel per auto als per spoor was het nog best ingewikkeld om aanwezig te zijn. Er is nog iemand onderweg. We hopen dat diegene ook nog komt, maar we zijn nu in ieder geval met een vaste kern die aan de slag kan. Ik heet dan ook de leden van de zijde van de Kamer welkom. Dat zijn mevrouw Koekkoek namens Volt, mevrouw Rajkowski namens de VVD en mevrouw Van Weerdenburg namens de PVV. Uiteraard heten we ook de Minister van Justitie en Veiligheid en haar staf van harte welkom. Dank daarvoor. Aan de orde is dus het debat over de Nederlandse cybersecuritystrategie. U heeft allen vier minuten spreektijd. Ik wilde voorstellen om vier interrupties in tweeën te doen, in beide termijnen. Mevrouw Koekkoek, ik geef u het woord.

Mevrouw **Koekkoek** (Volt):
Dank, voorzitter. Misschien is het goed om vooraf even te zeggen, ook richting de Minister, dat ik niet het hele debat hierbij kan blijven. Excuus. Er is exacte overlap met een ander debat hiernaast. Ik ga niet meteen wegrennen, maar dan weet u dat. Een vaste medewerker kijkt mee met de beantwoording. Alvast dank daarvoor.
Dan de Nederlandse cyberstrategie. Die vormt wat ons betreft een hele goede stap richting een digitaal weerbare maatschappij. Ik ben positief over de strategie en het actieplan, maar ik vind het ook belangrijk om de voortgang goed te kunnen controleren. Het actieplan is namelijk ambitieus, maar nog niet overal even specifiek. Dat is ook begrijpelijk. Daarom heb ik de vraag aan de Minister welke mogelijkheden zij ziet om de Kamer te informeren over de voortgang van het actieplan. Kan zij bijvoorbeeld begin 2023 een brief met een meer uitgebreide en concrete planning sturen?
Voorzitter. Ik heb twee inhoudelijke punten over de strategie. Het eerste punt gaat over de betrokkenheid van burgers. Het cybersecuritybeleid komt tot op heden namelijk voornamelijk tot stand via publiek-private samenwerking. We zijn zeker gebaat bij de kennis van de private sector over cybersecurity, maar de private sector heeft ook veel inspraak. In mijn optiek is cybersecurity niet alleen iets puur technisch, maar ook iets wat de samenleving aangaat. Daarom zou ik zeggen: burgers moeten juist veel inspraak hebben en vooraf meedenken. Er moeten waarden worden afgewogen. Dat vereist uiteindelijk uiteraard politieke keuzes. Daarom is mijn vraag: richten we ons met deze strategie niet te veel alleen op veiligheid? Houden we ook rekening met een behoefte aan bijvoorbeeld gebruiksgemak? Waar ligt de balans tussen privacy en veiligheid? Welke prijs is men bereid te betalen voor veiligheid? Dat is een vraag die we natuurlijk vaker zien als het over veiligheid versus andere waarden gaat. De actieve discussie over tegengestelde belangen wordt in mijn optiek te weinig gevoerd. Je wil namelijk de macht van de private sector beantwoorden met een bepaald soort tegenmacht. Daarom wil ik ervoor pleiten om burgers te betrekken bij het bepalen van zo'n cybersecuritystrategie.

Mijn vraag aan de Minister is of zij een brief kan sturen waarin deze afwegingen worden toegelicht en waarin zij uitlegt hoe zij burgers heeft betrokken en ook in de toekomst structureel... Ik zal even wachten.

De **voorzitter**:
Voor de kijkers thuis die het niet konden horen, zeg ik even dat de bel ging. Die gaat altijd een minuut lang bij aanvang van de plenaire vergadering, dus dat wilden we u allemaal niet aandoen via de microfoons. Vervolgt u uw betoog.

Mevrouw **Koekkoek** (Volt):
Ik ga even de vraag herhalen, anders is het een heel raar verhaal. De vraag is of de Minister een brief kan sturen waarin de afwegingen ten aanzien van privaat en publiek en met name het betrekken van burgers kunnen worden toegelicht en waarin zij uitlegt hoe burgers zijn betrokken en hoe zij in de toekomst burgers structureel wil betrekken bij het maken van dit soort keuzes.
Voorzitter. Dan mijn tweede punt, namelijk onze strategische autonomie. In de strategie staat dat bij digitale producten of diensten de risico's ten aanzien van spionage, beïnvloeding of sabotage en de statelijke actoren worden beoordeeld. Maar voor veel digitale diensten zijn slechts een paar alternatieven, die dan ook weer vergelijkbare risico's met zich meebrengen. Ik heb het bijvoorbeeld over software om tegelijkertijd samen te kunnen werken in dezelfde bestanden. Denk aan Google Drive of Microsoft Teams. Mijn vraag aan de Minister is of zij vindt dat wij moeten inzetten op het beter ontwikkelen van Europese alternatieven. Als het antwoord daarop ja is, hoe creëren we dan een ecosysteem waarin deze ontwikkeld gaan worden? Welke stappen moeten we hiervoor zetten? Of gaan we ervan uit dat diensten van elders, met name dus van de VS, zich aan onze regels zullen blijven aanpassen? Ik hoor graag hoe de Minister daarnaar kijkt. In hoeverre kunnen we naleving van onze regels ook controleren? Ik ben ook benieuwd naar de visie van de Minister op handhaving. Stel dat die alternatieven niet voorhanden zijn, hoe gaan we dan wel controleren dat onze eigen Europese waarden hier goed tot uiting komen?
Voorzitter. Ons cybersecuritybeleid is nog lang niet af. Nieuwe technologie leidt ook tot nieuwe vraagstukken. Elektronische deurbellen, robotstofzuigers en elektrische auto's: stuk voor stuk kunnen deze apparaten vanaf de volgende software-update een nieuwe microfoon of camera inschakelen, met gevolgen voor onze cybersecurity. Er wordt nu op Europees niveau gewerkt aan wetgeving hiervoor, maar Volt vraagt ook aandacht voor de handhaving. Hoe kijkt de Minister hiernaar? Staan we hierin sterk genoeg? Hoe gaan we de cybersecurity van al onze producten borgen, terwijl we ook de voordelen willen behouden van internationale handel? Omdat ik niet bij de beantwoording kan zijn, heb ik eigenlijk nog een alternatief. Mocht de Minister al deze vragen nog niet kunnen beantwoorden, wil ik haar heel graag vragen om met een plan te komen. Vandaar dat ik al een aantal keer om een brief heb gevraagd.
Dank, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Koekkoek namens Volt. Ik kijk even rond. Er zijn geen interrupties, dus ik geef het woord aan mevrouw Rajkowski namens de VVD.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Onze ziekenhuizen, banken, havens en het mkb worden dagelijks aangevallen. Deze digitale aanvallen zijn zo frequent en de gevolgen van een succesvolle aanval kunnen zo'n impact hebben op ons land en onze economie dat een omvangrijke aanpak nodig is. We willen

geen hapsnapbeleid maar stevige, hoge, dikke digitale muren met structurele aandacht voor het beschermen van Nederland tot op het hoogste niveau, zodat Nederlanders vooral kunnen genieten van de voordelen die digitalisering biedt. Daarom heeft de VVD dit debat ook aangevraagd. We praten hier niet voor het eerst over. In de afgelopen debatten heeft de VVD veelvuldig aangegeven dat we kwaadwillende landen buiten de deur moeten houden bij belangrijke aanbestedingen en dat we ons mkb moeten helpen om cybercriminelen buiten de deur te houden. Daar zien we ook een hoop van terug in deze strategie. Daar zijn we ook tevreden over.

Voorzitter. Sowieso zijn complimenten aan Onze Minister op hun plaats voor deze veelomvattende en ambitieuze strategie. Hiermee toont ze aan dat er een hoop gebeurt om Nederland veilig te houden en dat er degelijke plannen zijn voor de komende jaren. Dat is ook nodig, want de digitale dreiging is de afgelopen jaren gigantisch toegenomen. We worden alsmaar digitaler. Tegelijkertijd waarschuwden onze veiligheidsdiensten vorige week dat cyberdreigingen permanenter worden en Nederland steeds kwetsbaarder wordt. De Wetenschappelijke Raad voor het Regeringsbeleid gooit daar eigenlijk nog een schepje bovenop en zegt dat het steeds digitaler worden van onze samenleving ook betekent dat als het een keertje misgaat, we geen analoge alternatieven hebben.

Voorzitter. Dat is ook het hoofdpunt van mijn betoog. Wat doen we als het misgaat? Hebben we een plan B voor als de digitale pleuris uitbreekt? We maken ons hier als VVD zorgen over. De NCTV waarschuwde vorige week niet voor niets dat alle Nederlanders 48 uur thuis moeten kunnen overleven zonder internet, stroom en water. Alles is door digitalisering zo verknoopt geraakt met elkaar dat een succesvolle aanval op één organisatie ervoor kan zorgen dat Nederland in rap tempo als dominosteentjes richting een totale black-out gaat. Denk aan niet meer kunnen tanken, niet meer kunnen pinnen of niet meer een ziekenhuis kunnen bereiken. Daar moeten we op voorbereid zijn. Daar vroeg de VVD twee weken geleden naar in het vragenuur met de Staatssecretaris. Alleen, met de brief die daarop volgde, waren we er niet gerust op. Het is duidelijk dat de crisisplannen per sector klaarliggen. Dat is zeker al een goede eerste stap. Er is een crisisplan energie, een crisisplan Schiphol, een crisisplan Rotterdamse haven. Maar zoals ik al eerder zei, zijn deze sectoren wel degelijk met elkaar verbonden via de digitale snelweg. Een aanval op één sector kan leiden tot een aanval op alle sectoren. Hebben we dan iets om op terug te vallen als de digitale snelweg platligt? Is er wel een offlinealternatief? Als er iets uitvalt, is er dan een plan B?

Wat de VVD betreft moet er een nationaal digitaal crisisplan klaarliggen voor als het misgaat, met daarin de volgende drie punten. Eén. Analoge fallbackopties. Als alles digitaal is en eruit ligt, wat kunnen we dan wel? Het moet duidelijk worden welke vitale infrastructuur we via analoge opties draaiende moeten houden en wat daarvoor nodig is. Twee. Een digitale stresstest. Er moet geoefend worden met crisissituaties, zodat iedereen door alle bestuurslagen heen weet wat er moet gebeuren. Hier moeten dus ook de rijksoverheid, de veiligheidsregio's, Defensie en vitale sectoren zoals de energiesector en drinkwatervoorziening bij betrokken zijn. En drie. De kracht van het bedrijfsleven. Zorg ervoor dat in geval van nood ook personeel uit het bedrijfsleven tijdig bij kan springen. Zorg voor gescreende mensen bij die bedrijven die specifieke dreigingsinformatie kunnen ontvangen van inlichtingendiensten. Met deze informatie kunnen zij makkelijker cyberaanvallen afwenden en de benodigde veiligheidsmaatregelen nemen, en daarmee dus ook Nederland beschermen. Graag horen wij hoe de Minister tegen dit plan aankijkt.

Voorzitter. Ik zou natuurlijk heel graag nog uitgebreid willen ingaan op digitale vaardigheden in het onderwijs, het aanpakken van cybertuig en nog veel meer. Dat doen we een andere keer, maar ik heb nog wel een allerlaatste punt. Dat gaat over het maken van wetten. De ambities van

deze Minister in dit plan steunen we. Maar niet alles is te behalen zonder dat eerst in wetgeving om te zetten. De NIS 2 gaat over vitaal, maar wat doen we met niet-vitaal? Voor de integratie van het DTC en NCSC zal vast ook nog een of andere wet geregeld moeten worden. Graag dus een reactie van de Minister hoe zij voortvarend de benodigde wetstrajecten gaat starten.
Dank.

De **voorzitter**:
Dank u wel, mevrouw Rajkowski namens de VVD. U heeft een interruptie van mevrouw Van Weerdenburg, PVV.

Mevrouw **Van Weerdenburg** (PVV):
Ik vroeg me even het volgende af. Mevrouw Rajkowski geeft de Minister complimenten voor het plan. Ze zegt dat ze er een hoop in terugziet van wat de VVD de afgelopen tijd heeft ingebracht. Aan de andere kant verzoekt of eist ze een volledig plan B. Dat doe je meestal als je niet zo veel vertrouwen hebt in plan A. Het spreekt elkaar dus een beetje tegen. Wat zijn de elementen die vooral missen in deze securitystrategie volgens de VVD?

Mevrouw **Rajkowski** (VVD):
Dit geeft mij misschien ook de gelegenheid om het iets meer uit te leggen. De VVD vraagt niet om een plan B voor de hele cybersecuritystrategie. We zijn heel blij met wat erin staat. Het geeft ons overzicht, ook van wat de andere departementen doen. Dat is heel fijn voor onze sturende en controlerende taak. Het plan B gaat echt over het gebied van crisis. We zagen ook dat er allerlei crisisplannen zijn. Alleen, sommige crisisplannen zijn juist nog digitaal ingericht. Dan gaan we met een ander digitaal middel het systeem vervangen. Daar ligt bij ons precies de crux. We zien dat nog terugkomen niet in de plannen. Ik ben ervan overtuigd dat er al heel veel bouwstenen liggen, want er zijn sectorale crisisplannen. Dat werd ook in de brief aangegeven. De VVD is alleen op zoek naar de nationale kop erop. Als al die sectoren met dezelfde problemen te maken hebben, wie houdt dan het overzicht in Nederland, en dan specifiek wat betreft de analoge terugvalopties? We hebben geen praatpalen meer langs de weg, geld is digitaal et cetera. Wat is dan ons plan B?

De **voorzitter**:
Een vervolgvraag van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):
Mijn verwarring komt misschien door het feit dat we hier het plan bespreken om te voorkomen dat de digitale pleuris uitbreekt. Daar had ik misschien wat meer commentaar op verwacht van de VVD. Mevrouw Rajkowski gaat al een stap verder door te vragen: wat nou als dat faalt? Vandaar mijn verwarring. Kan ze daar nog heel even op ingaan?

De **voorzitter**:
Dank weer voor dit beeldende commentaar. Mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Fijn dat de term «digitale pleuris» blijft hangen. We hebben hier vaker met elkaar gezeten over cybersecurity. De VVD is elke keer met een plan gekomen. In april hadden we een vierpuntenplan. Zo zijn we elke keer met ideeën gekomen voor wat wij terug zouden willen zien in de cybersecuritystrategie. Daar zien we een hoop van terug. Sommige dingen kunnen misschien net wat scherper, maar wat ons betreft is het goed genoeg. Daar zijn we dus erg blij mee. We zijn gaan nadenken over het volgende. Honderd procent veiligheid bestaat niet. We kunnen niet voorkomen dat

er ooit een keer iets mis zal gaan. Op straat bestaat dat niet, maar ook digitaal niet. Toen dacht ik: we hebben nu het plan om te voorkomen dat criminelen of statelijke actoren binnenkomen, maar moeten we er dan misschien nu al naar kijken wat we doen als het dan toch een keertje lukt? Dat was voor ons de strategie van dit debat.

De **voorzitter**:
Dank u wel, mevrouw Rajkowski. Ik zie mevrouw Van Weerdenburg knikken. Ik zie verder geen interrupties meer. Dan geef ik mevrouw Van Weerdenburg het woord voor haar eigen inbreng namens de PVV.

Mevrouw **Van Weerdenburg** (PVV):
Dank u wel, voorzitter. Ik voer vandaag het woord namens de PVV en ook namens BVNL, oftewel Groep Van Haga. Beide fracties onderstrepen het belang van een heldere cybersecuritystrategie waarin ieders taken en verantwoordelijkheden duidelijk zijn. Met een robuuste cybersecurityinfrastructuur waarin de lijnen zo kort mogelijk zijn en de informatievoorziening supersnel. Want in een crisissituatie is flexibiliteit en snelheid van levensbelang. De Cyber Security Raad en de Onderzoeksraad voor Veiligheid hebben in lijvige rapporten al aangegeven dat het huidige cybersecuritylandschap gefragmenteerd is met gaten en veel te veel overlap, waardoor tijdens een crisis veel tijd wordt verloren en onnodige risico's worden gelopen. Het werd zelfs «een lappendeken» genoemd. De PVV en BVNL zijn blij dat de nieuwe cybersecuritystrategie er nu eindelijk ligt, maar we betwijfelen of dit een adequaat antwoord is op die kritiek. Vooral de lengte van het tijdspad baart ons zorgen, want we hebben toch samen allang geconstateerd dat de digitale dreiging rap toeneemt en dat we onze zaken eigenlijk gisteren al op orde hadden moeten hebben? Hoe kan de Minister dan 2026 hanteren als deadline voor het invullen van alle randvoorwaarden om alle organisaties snel en adequaat te bereiken? Dat moet toch veel sneller? Ook de OVV is teleurgesteld hierover en roept op om te versnellen, omdat de kloof tussen cyberdreiging en weerbaarheid continu groter wordt.
De stap om informatiedeling binnen het landelijk dekkend stelsel van cybersecuritysamenwerkingsverband LDS te verbeteren door de integratie van NCSC, DTC en CSIRT-DSP tot één organisatie, dus een nationaal CSIRT, juichen wij toe. Wij vragen ons wel af of die integratie niet wat sneller kan. We hebben het er al eerder over gehad met de Minister. Die organisaties werken immers nu ook al nauw samen. Welke mogelijkheden tot versnelling ziet de Minister? Begrijpen wij uit de stukken goed dat het nieuwe CSIRT zowel onder het Ministerie van JenV als onder het Ministerie van EZK valt? Over die governance maken wij ons namelijk ernstig zorgen.
Voorzitter. Helaas is dat een terugkerend onderwerp in deze commissie. In de zoektocht naar de verantwoordelijke bewindspersoon, degene die erover gaat, krijgen we steeds meer hybride varianten voorgeschoteld. Zo lezen we nu in de nationale cybersecuritystrategie dat de Minister van JenV coördinerend bewindspersoon is voor cybersecurity en verantwoordelijk is voor de aanpak van cybercrime, en dat zij regie voert op de uitvoering van deze strategie en de monitoring daarvan. Echter, voor het behalen van de cybersecuritydoelen houdt iedere partij zijn eigen taken en verantwoordelijkheden. En o ja, er is ook nog een nauwe samenhang met de inzet van het kabinet op digitalisering onder regie van de Staatssecretaris Koninkrijksrelaties en Digitalisering, zoals uiteengezet is in de hoofdlijnenbrief.
Ik heb het echt vier keer moeten lezen, maar de Minister van JenV is dus coördinerend bewindspersoon die regie voert op de uitvoering en monitoring van deze strategie, maar ze is niet verantwoordelijk voor het behalen van de doelen. Wat betekent dat nou eigenlijk? Iedereen kent de term «creatief boekhouden», maar volgens mij is hier echt sprake van

creatief besturen, en dan niet in positieve zin. Als iedereen er namelijk over gaat, is er dus niemand echt de baas. Dan is er dus ook geen direct verantwoordelijke als het een keer misgaat. Mevrouw Rajkowski noemde dat de «digitale pleuris». We houden die term er gewoon in. Ik verzoek de Minister om goed te verduidelijken wat regie voeren precies inhoudt en wat het betekent om coördinerend bewindspersoon te zijn van iets. Heeft zij doorzettingsmacht richting andere departementen? Tot hoever reikt haar besluitvormende bevoegdheid, ook als het gaat om eventuele aanpassingen aan deze strategie? Moet dat dan weer langs alle overlegtafels, vergaderclubjes en klankbordgroepen? Dan snap ik dat belachelijk lange tijdspad een stuk beter. Wat de PVV en BVNL betreft kan de Minister in dat geval direct terug naar de tekentafel, want zo gaat dit niet werken. Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, mevrouw Van Weerdenburg, voor uw inbreng namens de PVV. Ik zie dat inmiddels ook mevrouw Dekker-Abdulaziz is aangeschoven namens D66. Welkom. U heeft het keurig getimed, want u krijgt meteen het woord voor uw inbreng. Mevrouw Dekker-Abdulaziz.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank, voorzitter. Dank ook dat ik wat later binnen kon komen. De komst van deze Nederlandse cybersecuritystrategie zou ik echt willen markeren als een belangrijk moment. Ik kan een lange lijst maken van dingen waar ik blij van word in deze strategie, maar dat ga ik niet doen. Woorden op papier zijn namelijk niet genoeg. Het er hier over hebben is ook niet genoeg. Of Nederland digitaal veiliger wordt, staat of valt met de uitvoering. Daar zit echt mijn angst. Het mag niet zo zijn dat de realiteit de bestuurlijke maximumsnelheid inhaalt, terwijl de basis van onze kenniseconomie langzamerhand onder onze voeten verdwijnt. Als onze bedrijfsgeheimen via hacks gestolen worden, zal Nederland als kennisland langzaam maar zeker irrelevant worden. Dat bedreigt onze banen en onze welvaart. Economische spionage is een zinkgat. Je hebt het pas door als je wegzakt, en dan is het te laat. Dinsdag kwam de OVV nog met een forse waarschuwing dat de dreiging groter is dan de weerbaarheid, dat partijen moeten versnellen en dat het tempo omhoog moet. Plannen zijn leuk, snelheid is beter. Vindt de Minister een doorlooptijd tot en met 2026 voor 20 van de 23 acties op het gebied van statelijke actoren niet veel te mager? Komen de cybercapaciteiten van Defensie dan niet te laat? Komen de kennis en kunde bij het OM niet te laat, net als de informatiedeling binnen de EU en in NAVO-verband? Hoe dragen de acties in dit plan nou bij aan de doelen die we willen bereiken, aan een digitaal veiliger Nederland? Zou de Minister in een brief per actie kunnen aangeven welke effecten wij kunnen verwachten?
Voorzitter. Voor het beschermen van onze kennis is encryptie cruciaal. Het is goed dat we inzetten op security bij default, maar tegelijkertijd wil de Minister haar zoektocht naar een eenhoorn om door de achterdeur te komen tot nu toe niet opgeven. Kennis beschermen en tegelijkertijd encryptie ondermijnen? Dat is als het vleugellam maken van een vogel en hem dan uit laten vliegen. Kan de Minister toezeggen dat zij deze zoektocht staakt?
Voorzitter. Dit brengt mij bij de visie voor 2026 inzake het NCSC, het DTC en het CSIRT-DSP. Veel afkortingen, sorry. Eerder vertelde de Minister dat er nog veel moest gebeuren. Zijn we nu al verder? Is er duidelijkheid over de bestuurlijke verantwoordelijkheid voor de nieuwe organisatie? Kan de Minister toezeggen het tempo op te voeren opdat men in 2024 klaar is? Waar de verantwoordelijkheid hiervoor ook ligt, dit dossier raakt zo veel beleidsterreinen en beleidslagen dat bestuurlijke samenwerking bij de uitvoering cruciaal is, tussen ministeries onderling, maar ook met gemeenten en staten. Gemeenten staan het dichtst bij onze inwoners en

hun problemen, maar moeten het tegelijkertijd regelmatig doen met maar 0,5 fte voor cybersecurity, zoals de gemeente Hof van Twente, waar het wachtwoord voor het beheeraccount «Welkom2020» was en de firewall werd opengezet voor iedereen. Kosten voor de samenleving: ruim 4 miljoen euro. Hoe denkt de Minister dat gemeenten en waterschappen met 0,5 fte de grote ambities van het Rijk waar kunnen maken? Dat aspect werd niet alleen door ons gemist, maar bijvoorbeeld ook door de VNG. Ook de Europese samenwerking zou wat ons betreft nog sterker en nog sneller kunnen. Het Europees agentschap voor cybersecurity, ENISA, ontbreekt bijvoorbeeld volledig. Zou de Minister dat hier recht kunnen zetten door alsnog op zijn rol in te gaan? Want als de strategie te weinig Europees is, hoe moet die dan de wereld en de dreigingen buiten Europa aankunnen? Kan de Minister op dat gebied ook nog ingaan op de NIS2-richtlijn? Als er straks Europese veiligheidsstandaarden komen voor apparaten die zijn aangesloten op het internet, hoe gaan we dan om met apparaten van buiten Europa?
Ik kijk uit naar de antwoorden van de Minister. Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Dekker-Abdulaziz. Mevrouw Van Weerdenburg wil u interrumperen. Mevrouw Van Weerdenburg, PVV.

Mevrouw **Van Weerdenburg** (PVV):
Een mooi pleidooi voor het behoud van encryptie. Daar sluit ik mij heel graag bij aan namens de PVV en BVNL. Ik had even een vraag over de zorgen die mevrouw Dekker uitte over de governance, over de bestuurlijke verantwoordelijkheid, want die delen wij ook. Het is eigenlijk een soort tegenstelling: bij een acute dreiging moet je heel snel kunnen handelen, maar aan de andere kant is alles belegd in overlegtafels en werken alle ministeries samen. Nou ja, het is eigenlijk de discussie die we hebben gevoerd: moeten we één Minister voor Digitale Zaken hebben die snel kan schakelen en doorzettingsmacht heeft? Hoe ziet mevrouw Dekker dat bij deze strategie? Is die wendbaar, flexibel en snel genoeg?

Mevrouw **Dekker-Abdulaziz** (D66):
Dank voor deze vraag. Het probleem met de bestuurlijke governance is iets wat wij ook wel zien. Wij zien dat deze strategie niet een-op-een aansluit op de hoofdlijnenbrief en dat de acties niet altijd acties zijn, maar wel plannen. Dat zien wij wel. Wij vinden het eigenlijk wel goed dat in de actieplannen voor cybersecurity de verschillende ministeries verantwoordelijk zijn voor hun eigen stukje. Ik neem dan aan dat deze Minister nog steeds de coördinerende bewindspersoon is voor cybersecurity en dat dat de Staatssecretaris voor Digitale Zaken dat is voor de rest van de digitale zaken.

De **voorzitter**:
Dank u wel, mevrouw Dekker-Abdulaziz. Er is ook nog een interruptie van mevrouw Rajkowski van de VVD. Mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Ik hoor mevrouw Dekker zeggen: de strategie kan nog wat Europeser. Het zal u niet verrassen dat ik op sommige dossiers wel wat Europa-sceptisch ben, maar op het gebied van digitalisering zie ik dat Europa eigenlijk heel veel doet. Vanuit Europa komt allerlei wetgeving op Nederland af. Ik ben er echt van overtuigd dat Nederland daardoor veiliger gaat worden. Alleen, soms vind ik het wel spannend of iedereen, zoals gemeenten, het inderdaad mee kan maken. Ik ben dus nog een beetje op zoek naar wat er volgens D66 nog verder Europees zou moeten gebeuren.

Mevrouw **Dekker-Abdulaziz** (D66):

Dat betreft de twee dingen die ik eerder in mijn betoog heb gevraagd: ingaan op bijvoorbeeld het Europees agentschap voor cybersecurity, ENISA, dat geen rol heeft in deze strategie, en ingaan op de NIS2-richtlijn, die er ook wel gaat komen. Hoe gaan we hiermee dan om bij de visie, maar ook bij de actiepuntenlijst?

De **voorzitter**:
Dank u wel. Ik ziet dat u de vraag naar tevredenheid heeft beantwoord. Daarmee zijn we aan het einde gekomen van deze termijn van de Kamer. De Minister heeft aangegeven ongeveer 25 minuten nodig te hebben. Ik kijk even naar de klok. Ik stel gewoon voor om dat af te ronden en te schorsen tot 11.00 uur. Daarna volgt de beantwoording. Ik schors de vergadering.

De vergadering wordt van 10.34 uur tot 11.01 uur geschorst.

De **voorzitter**:
Aan de orde is het commissiedebat over de Nederlandse cybersecuritystrategie. We hebben net de eerste termijn van de Kamer gehad. Ik wil nu graag de Minister verzoeken om te beginnen met haar termijn en de beantwoording van de vragen. De Minister.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Allereerst wil ik u en uw collega-Kamerleden graag danken voor de uitnodiging om in dit debat over de Nederlandse cybersecuritystrategie te spreken. De nieuwe cybersecuritystrategie is tot stand gekomen met echt een brede betrokkenheid van vele publieke, private en maatschappelijke organisaties. Het lijkt mij gepast om te beginnen met een woord van dank aan hen voor hun bijdrage. Er zit echt intens veel werk in document. Dus dank.
Ik zou ook graag dank willen zeggen voor de snelle behandeling van de Wet beveiliging netwerk- en informatiesystemen. Door deze nieuwe wet, die per 1 december in werking is getreden, heeft het Nationaal Cyber Security Centrum een ruimere bevoegdheid om dreigings- en incidentinformatie te verstrekken. Daardoor kan het Nationaal Cyber Security Centrum bijvoorbeeld bedrijven waarvoor geen zogenaamde schakelorganisatie is, nu rechtstreeks informeren bij een impactvolle cyberaanval.
Voorzitter. Zoals het Cybersecuritybeeld Nederland 2022 laat zien, staat de maatschappij voor een grote opgave op het gebied van cyberweerbaarheid. We zien steeds meer cyberaanvallen door andere landen en we zien dat cybercriminelen grote, digitale schade kunnen aanrichten. Dat vraagt om een strategie die hierbij aansluit. Het actieplan en de strategie laten zien dat het kabinet zich er in grote mate voor wil inzetten om onze maatschappij op de lange termijn digitaal weerbaar te houden. Samenwerking met private partijen en de wetenschap is daarbij van essentieel belang voor de uitvoering van de strategie.
Voorzitter. Aanvankelijk had ik de vragen en antwoorden in mapjes verdeeld, maar uiteindelijk hebben we één mapje gemaakt: de strategie. Het komt dus allemaal hierin terug. Net, tijdens de schorsing, leek ons de volgorde logisch, maar het loopt dus door elkaar. Dat geef ik de Kamerleden alvast mee, zodat zij niet denken dat een vraag misschien al beantwoord is en daaraan een interruptie verspillen.

De **voorzitter**:
Misschien nog één ding voor de Minister. Ik denk dat u terecht wijst op de Nederlandse strategie. Die is toch ook op de website te vinden?

Minister **Yeşilgöz-Zegerius**:
Zeker.

De **voorzitter**:
Dat voor de geïnteresseerde kijkers. Volgens mij is die zeer lezenswaardig.

Minister **Yeşilgöz-Zegerius**:
Ik heb er hier nog een paar liggen. Mocht iemand nog kerstcadeaus zoeken voor thuis: deze kan meegenomen worden.
Voorzitter. Ik begin met vragen, in dit geval van de PVV en D66, over een snellere implementatie en acties van de strategie. Volgens mij zei mevrouw Van Weerdenburg letterlijk of in ieder geval iets van: «We gaan toch niet wachten tot 2026? Stel dat zich daarvoor dingen voordoen. Het is toch urgent? Wat gaan we doen?» Ik denk dat het goed is om eerst te benadrukken dat de looptijd van alle activiteiten bij elkaar wel tot 2026 is, maar dat we vóór de strategie al bezig waren met de actielijnen. We zijn daar nu mee bezig en we blijven daarmee bezig. In de strategie staan volgens mij meer dan 150 acties. Het is niet zo dat dat allemaal in 2026 een keer is opgepakt. Integendeel, want ik deel volledig de opvatting dat het superurgent is dat wij die acties zo snel mogelijk uitwerken. Zoals gezegd, zitten we er middenin.
Tegelijkertijd kunnen de cybersecuritymaatregelen alleen succesvol en effectief zijn als die maatregelen in publiek-privaat verband, in Europees verband en op nationaal niveau worden uitgewerkt. Sommige dingen kosten om die reden meer tijd, maar dan sta je natuurlijk niet stil. Het is ook van essentieel belang dat de uitvoerende organisaties in staat zijn om die maatregelen uit te voeren en te handhaven. Uiteraard is dat een zorgvuldig proces. Soms vereist het wetgeving – daar kom ik straks op terug – en juridische grondslagen. Die elementen kosten tijd. Die heb je daarvoor nodig. Ik zei al dat diverse acties al in gang zijn gezet. Ik noem een paar voorbeelden, maar ik zal ze niet allemaal noemen, voorzitter. We zijn bijvoorbeeld, als vervolg van de Cyber Intel/Info Cell, begonnen met het ontwikkelen van een publiek-privaat samenwerkingsplatform om informatie over aanwezige cyberincidenten sneller, effectief en breder te delen. Het Nationaal Cyber Security Centrum werkt intensief aan het verbeteren van de samenwerking met de zogenaamde schakelorganisaties uit het landelijk dekkend stelsel. En, zoals gezegd, is recent ook de Wet beveiliging netwerk- en informatiesystemen aangepast. Dat zijn allemaal voorbeelden van zaken die ook in de strategie staan en waar we gewoon volop mee bezig zijn.

De **voorzitter**:
Voordat u uw betoog vervolgt, is er een interruptie van mevrouw Dekker-Abdulaziz, D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank voor de antwoorden van de Minister. We snappen ook wel dat een aantal dingen al begonnen zijn. We zien de actielijst van 2022 tot 2026, maar we weten eigenlijk niet wanneer wat is gedaan. En dan kan de Tweede Kamer niet echt sturen op welke resultaten dan zijn geboekt, volgend jaar en in 2024. Is de Minister bereid om ons desnoods per brief te laten zien wanneer wat wordt verwacht? Dan kunnen we daarop sturen.

Minister **Yeşilgöz-Zegerius**:
Sterker nog, we hebben met elkaar afgesproken dat we na de vaststelling van de strategie, wat we nu aan het doen zijn, binnen een jaar met een rapportage, een update, komen waaruit blijkt hoe al die stappen eruitzien. Ik zou u willen vragen dat tempo aan te houden, zodat alle inzet gericht kan worden op het realiseren van al die acties en ik u jaarlijks op de hoogte kan houden. U kunt daar dan weer alles van vinden.

De **voorzitter**:
Dank u wel. Vervolgt u uw betoog.

Minister **Yeşilgöz-Zegerius**:
Ik had een vraag van de PVV en D66 over een specifiek punt uit het actieplan: kan de integratie van het Digital Trust Center en het Nationaal Cyber Security Centrum niet sneller en hoe ziet de governance eruit? Het doorlopen van het proces om die organisaties compleet te integreren kost tijd. Dat heeft er ook mee te maken dat je moet bekijken of het juridische kader dat we nu hebben, daarvoor volstaat of dat daar een andere grondslag voor nodig is. Dat moet zorgvuldig gebeuren en dat kost tijd. Ik kan daarom nu nog niet de toezegging doen dat het in een bepaald jaar, bijvoorbeeld 2024, volledig rond zal zijn. Maar ook hierbij geldt absoluut dat, waar mogelijk, activiteiten binnen het proces wel eerder zullen worden uitgevoerd. Dat zijn we nu al aan het inrichten. Die samenwerking gaat daar waar mogelijk natuurlijk wel plaatsvinden. De einddatum is dus weer de datum waarop de organisaties volledig geïntegreerd moeten zijn, met de wettelijke en juridische onderbouwing en de grondslag die je daarbij nodig hebt, maar die heb je natuurlijk niet per se voor alles nodig. Zo werken nu al medewerkers van de operatie van het Digital Trust Center samen met medewerkers van de operatie van het Nationaal Cyber Security Centrum en noem maar op. Alles wat kan, wordt al volop in beweging gezet, ook om ervoor te zorgen dat de grondslag stevig is.
Ik houd deze volgorde vast, voorzitter.
Dan een vraag van D66. Volgens mij was het D66. Of was het de PVV? Ja, ik had het toch goed. Hoe denkt de Minister dat de gemeenten en waterschappen met niet zoveel mensen toch de ambities van het Rijk waar kunnen maken? Dit is natuurlijk wel een heel erg legitiem punt. Denken dat je het hier kunt vaststellen en dat gemeenten en waterschappen het dan zomaar kunnen uitvoeren: zo zou het niet werken. Individuele gemeenten, provincies en waterschappen worden op verschillende wijzen ondersteund. Die ondersteuning wordt bijvoorbeeld gegeven door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, door de eigen koepelorganisaties zoals de VNG of bijvoorbeeld door het Ministerie van Infrastructuur en Waterstaat als moederdepartement van de waterschappen. Daar is dus heel veel aandacht voor. Specifiek werkt de Vereniging van Nederlandse Gemeenten via de gemeentelijke Agenda Digitale Veiligheid aan de digitale weerbaarheid van gemeenten. Daar is dus een apart programma voor. Verder heeft het Ministerie van Infrastructuur en Waterstaat specifiek voor de waterschappen het programma Versterken Cyberweerbaarheid in de Watersector. Wat we dus eigenlijk doen, is interbestuurlijk met onze medeoverheden de krachten bundelen om te voorkomen dat iedereen op eigen wijze het wiel moet uitvinden of zelf moet gaan uitpuzzelen hoe dit te doen. Misschien is het goed om hieraan het volgende toe te voegen. Om gezamenlijk door te pakken op de weerbaarheid van gemeenten werkt mijn ministerie met het Ministerie van Binnenlandse Zaken, de Vereniging van Nederlandse Gemeenten en de grootste vier gemeenten aan afspraken voor de komende jaren. Die komen in een bestuurlijk convenant en die zullen we ook volgende week bekrachtigen. Er is dus veel ondersteuning op allerlei niveaus, met expliciet aandacht voor de kleinere gemeenten die niet veel capaciteit en expertise hebben. Ook voor hen is er dus veel ondersteuning.

De **voorzitter**:
Er is een interruptie van mevrouw Dekker-Abdulaziz, D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Dank aan de Minister voor het antwoord. Het klinkt inderdaad wel als veel. De verschillende ministeries doen allemaal iets. Fijn om te horen dat er een bestuurlijk convenant komt. Maar bij wie kan een gemeente die een probleem heeft, dan terecht? Moet zij dan met de VNG bellen of moet zij

dan met het ministerie bellen? Kan de Minister dat even wat meer toelichten?

Minister **Yeşilgöz-Zegerius**:
Dan kunnen ze terecht bij de Informatiebeveiligingsdienst van de VNG. Daar is dus een specifiek loket voor.

Mevrouw **Dekker-Abdulaziz** (D66):
Het is fijn om te weten dat ze bij de VNG terechtkunnen. Ik hoorde ook dat de VNG goed met JenV samenwerkt om de zaken te regelen. Dank.

Minister **Yeşilgöz-Zegerius**:
Absoluut. Er is echt heel veel aandacht voor dit punt. Ik sluit niet uit dat we dit de komende tijd gewoon scherp moeten houden en elke keer moeten kijken waar eventueel wel gaten vallen of zich knooppunten voordoen, maar daar hebben we samen met de VNG heel veel aandacht voor.
Dan de VVD, eigenlijk over plan B. Stel dat er toch dingen misgaan, hebben we dan genoeg terugvalopties, analoge terugvalopties of anderszins, als een aanval plaatsvindt die onze vitale infrastructuur en processen raakt en digitale «steunpilaren» onderuithaalt? Een belangrijk doel binnen pijler één van de Nederlandse cybersecuritystrategie is dat we voorbereid moeten zijn op dit soort zaken, op digitale incidenten en crises. Mocht dat gebeuren, mocht zo'n vitaal proces uitvallen, dan is het erg belangrijk dat we voldoende terugvalopties hebben. In eerste instantie dienen organisaties de afweging op het gebied van terugvalopties en back-ups mee te nemen in de eigen risicoanalyse en crisisplannen. Bij incidenten met een nationale uitstraling is ook regie vanuit de overheid gewenst. Voor de verschillende vitale processen wordt periodiek de weerbaarheid in kaart gebracht, waarbij er aandacht is voor maatregelen om de continuïteit van het vitale proces te verzekeren. Ik noem bijvoorbeeld alternatieve werkwijzen om voorraden in te vullen ongeacht de oorzaak van de uitval. De rijksoverheid heeft vooral bij systemen met fysieke componenten een goed beeld van terugvalopties voor essentiële diensten. Een voorbeeld daarvan is het inrichten van digitale radiozenders op standalonegebruik, dus op analoog gebruik. Een ander voorbeeld is het continu bemensen van politiebureaus en brandweer- en ambulanceposten als noodmeldpunt in het geval hulpdiensten via 112 onbereikbaar zijn.
Zo heb je steeds voor elk van dit soort onderdelen een apart plan liggen. Maar ik moet eerlijk zijn: een analoge terugvaloptie is niet altijd een reëel alternatief voor een bepaalde functie. Neem nou ver ontwikkelde gedigitaliseerde processen. Daarbij kan men bijvoorbeeld vanwege de hoge kosten niet terugvallen op dat soort analoge opties. Je kan denken aan mondiaal internet. Ja, dan houdt dat gewoon in die zin op. Dan moet je weer specifiek kijken hoe je dat invult, zoals ik dat net zei over 112. Nou, het internet is misschien niet het beste voorbeeld, maar ik zie dat mevrouw Rajkowski kan volgen wat ik hier bedoel. Dat blijkt ook uit het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid over het voorkomen van digitale ontwrichting.
Ik heb er nog eentje van mevrouw Rajkowski. Zij vraagt of er dan ook een nationaal crisisplan is. Het is prima dat we daar allemaal over hebben nagedacht, maar waar komt het bij elkaar? Fijne vraag, want nog voor het einde van dit jaar – dat is dus al bijna – zal ik u het herziene landelijk crisisplan digitaal aanbieden. We hopen het nog op tijd voor de kerst vast te kunnen stellen. Daarin is vastgelegd hoe publieke en private organisaties in Nederland zich moeten voorbereiden op en moeten handelen tijdens zo'n crisis door cybersecurityincidenten of zaken groter dan een incident. Met het landelijk crisisplan digitaal zal vervolgens geoefend worden tijdens ISIDOOR IV. Die oefening zal eind 2023/begin 2024

plaatvinden. In andere debatten hebben we het er ook over gehad dat de kracht van ISIDOOR juist is dat het een brede, cross-sectorale oefening is, waarbij het scenario over verschillende sectoren heen gaat, zodat het die sectoren dus weer bij elkaar brengt. Dan kijken we ook naar een goede balans tussen publiek en privaat en naar ieders verantwoordelijkheden. Dan ben ik bij encryptie. D66 zei: het is cruciaal, maar de Minister blijft op zoek naar die eenhoorn. Laat ik die eenhoorn los? Nee. Dat is ook wel een heel heftige toezegging, hoor: ophouden met zoeken naar eenhoorns. Nee, daar houden we niet mee op, maar het is natuurlijk wel een serieuze vraag, en ik snap die ook. Als Kamerlid heb ik me ook altijd uitgesproken voor sterke encryptie. Als Minister heb ik niet alleen dat standpunt; de Kamer is er ook nogal duidelijk over en dan heb ik mij daar dus ook naar te gedragen. Het gaat ook over de ontwikkeling van encryptie en het behoud ervan. De beschermende waarde van encryptie om te voorkomen dat criminelen toegang krijgen tot persoonlijke gegevens staat dus niet ter discussie. Dit is natuurlijk een domein waarop heel veel ontwikkelingen elkaar heel snel opvolgen. Dat maakt dat je heel goed voorbereid moet zijn op van alles, waar we het zojuist over hadden, maar ook dat we altijd hoopvol zijn dat er wél een eenhoorn langskomt waarover iedereen zegt: nou, die hadden we nooit zien aankomen. Dat betekent dus dat we altijd op zoek zijn naar een oplossing waardoor bevoegde autoriteiten op een gerichte en rechtmatige manier toegang kunnen krijgen tot gegevens. Maar de uitspraak van de Kamer en hoe ik daarin zit: dat is helder. Daar tornen we niet aan. Op het moment dat we denken «hé, maar hier is een nieuw iets», breng ik het in de Kamer in. Dat heb ik met de Kamer afgesproken. Dan hebben we het er met elkaar over en dan kunnen we wegen of we het inderdaad als zodanig beschouwen. De eerlijkheid gebiedt te zeggen dat ik dat niet heb. Er is dus nog geen eenhoorn die ik hier op tafel leg.

De **voorzitter**:
Kijk eens aan. Aan de mensen op de publieke tribune die net binnenkwamen: u bent hier inderdaad bij een debat over cybersecurity en niet bij een debat over eenhoorns. Het gaat inmiddels over encryptie.
Minister, u heeft twee interrupties. De eerste is van mevrouw Van Weerdenburg, PVV, en de tweede van mevrouw Dekker-Abdulaziz.

Mevrouw **Van Weerdenburg** (PVV):
Toch nog heel even over die eenhoorn. Kan de Minister de Kamer toezeggen dat Nederland zich niet zal committeren aan wetgeving, eventueel zelfs uit Brussel, die gebaseerd is op die nog niet gevonden eenhoorn? De Minister weet wel dat ik doel op de CCAM regulation, die de bal doorschuift naar andere partijen en die dan maar moeten verzinnen waar die eenhoorn vandaan komt. Kan de Minister toezeggen dat Nederland zich daar niet aan zal binden?

Minister **Yeşilgöz-Zegerius**:
Dat heb ik vastgelegd. Dat staat in brieven en dat is ook de uitvoering van de motie-Van Raan. Dus zo zitten wij daarin. Ik heb begrepen dat Eurocommissaris Johansson – althans, ik heb het zelf aangeboden, maar ik heb begrepen dat ik dat niet kon aanbieden en dat zij het zelf moest aanbieden – meer dan bereid is om hier eens langs te komen en uit te leggen hoe zij dat ziet en waar zij die ruimte ziet. Het standpunt van de Nederlandse regering komt in die zin helemaal overeen met wat de Kamer heeft gewenst en dat hebben we ook vastgelegd.

De **voorzitter**:
Een vervolgvraag van mevrouw Van Weerdenburg.

Mevrouw **Van Weerdenburg** (PVV):

Ja, toch nog even. Hangen we daar dan ook een opt-out aan? Want in Brussel worden wel vaker dingen beslist waar Nederland niet aan mee wil doen, maar op een gegeven moment word je gewoon overruled. Dan is het toch geldend recht en dan hebben we dat in te voeren. Kan de Minister toezeggen dat Nederland op dat moment, mocht dit allemaal zo gebeuren, van tafel opstaat en zegt: wij niet?

Minister **Yeşilgöz-Zegerius**:
Er zijn meer landen waarin dit vraagstuk zich afspeelt. Ik heb met de Kamer afgesproken dat ik kijk of er wat dat betreft meer landen zijn, zodat je niet in je eentje staat. We kijken daar dus naar. Dat moment is er nog niet, maar het standpunt van Nederland is heel erg helder. De toezegging staat dat we de Kamer van het hele proces, stap voor stap, op de hoogte houden, en die wil ik hier graag onderstrepen. De wet gaat over de vraag hoe je er op een efficiënte manier voor kunt zorgen dat je bijvoorbeeld online kinderporno tegengaat. Daar heeft de Kamer ook zelf aandacht voor gevraagd. Ook dat willen we met z'n allen. Tegelijkertijd willen we dat de middelen die daarvoor worden ingezet, passen bij hoe we daarin staan. En dat is bijvoorbeeld het niet doorbreken van encryptie. In die balans ben ik nu aan de slag. En «balans» is dan een balans in die zin dat ik wel wil dat we sneller kunnen komen bij de gegevens die we willen hebben van de criminelen en misbruikers – want ook dat is een opdracht van de Kamer – maar niet dat we daarbij encryptie doorbreken. Ik blijf dus in gesprek en op zoek naar medestanders in Europa. Ik blijf de Kamer informeren, en dan bouwen we het zo op.

De **voorzitter**:
Misschien voor de volledigheid: dit onderwerp wordt ook nadrukkelijk gevolgd in de commissie voor Justitie en Veiligheid. Er komt vanmiddag een debat.

Mevrouw **Dekker-Abdulaziz** (D66):
Binnenkort vindt ook een tweeminutendebat plaats of een SO dat volgens mij door Van Raan is aangevraagd. Maar mijn vraag gaat meer over het principe van het zoeken naar een eenhoorn. Ik snap dat de Minister zegt: ons standpunt is hetzelfde als dat van de Kamer; dat dragen we uit en dat gaan we uitvoeren. Maar als wij op de een of andere manier encryptie voor de bevoegde autoriteiten verzwakken, dan is er altijd een kwetsbaarheid die iemand die niet bevoegd is, kan vinden. Uiteindelijk zijn we dan met z'n allen niet veilig. Hoe kijkt de Minister dan daartegen aan?

Minister **Yeşilgöz-Zegerius**:
Met dit soort complexe vraagstukken moet je, denk ik, niet heel veel in de als-danscenario's gaan. De opdracht van de Kamer is helder: encryptie wordt niet verbroken. Zoeken betekent ook dat de mogelijkheid bestaat dat wordt geconstateerd dat er geen proportionele oplossing is. Maar in deze zich snel ontwikkelende wereld – dat geldt zeker voor de wereld van technologie – zou ik het wel een gemiste kans vinden als we zeggen dat we nooit open zullen staan voor oplossingen die opeens wel langs kunnen komen. Het kan zijn dat ik die in mijn tijd als Minister niet ga meemaken en mijn opvolgers ook niet. Dat kan ook een constatering zijn. Het is niet dat ik denk: nou, volgende week hebben we zo'n gesprek. Volgens mij is het goed als u mij vooral vraagt daar wel altijd naar op zoek te zijn, want de reden waarom een achterdeur wordt gezocht – nog even los van encryptie – is wel een hele wezenlijke. Dus die balans. Het is duidelijk welke instrumenten we niet gaan inzetten.

De **voorzitter**:
Een vervolgvraag van mevrouw Dekker-Abdulaziz. Overigens heeft u inmiddels al drie interrupties gepleegd.

Mevrouw **Dekker-Abdulaziz** (D66):
Ja, dit is mijn vierde. Het is mijn laatste.
Dank voor het antwoord. Ik wil dan alleen zeggen dat wij altijd tegen het verzwakken van encryptie zijn, ook al is de reden heel erg goed. Want het is altijd een risico. Maar dat weet de Minister wel.

De **voorzitter**:
Dank u wel. Vervolgt u uw betoog.

Minister **Yeşilgöz-Zegerius**:
Ja. Dan was ik bij de vragen van Volt over digitale autonomie. Het ging over het inzetten op Europese alternatieven voor software en op een Europees ecosysteem voor de ontwikkeling daarvan. Investeringen in de digitale transitie dragen bij aan de Europese concurrentiekracht en een digitale autonomie van de EU. Daarom investeren we ook in hoogwaardig onderwijs, in excellent onderzoek en in innovatie, om technologisch leiderschap te behouden. Het kabinet zal in de loop van volgend jaar met de nadere invulling van de digitale autonomie van de digitale economie en infrastructuur komen.
D66 stelde ook vragen in het kader van de Europese samenwerking. Waarom ontbreekt ENISA, het Europees cybersecurityagentschap, in de strategie? In de Nederlandse cybersecuritystrategie hebben we aangegeven dat maatregelen alleen maar effectief kunnen zijn als ze ook in internationaal verband worden uitgewerkt. De Europese Unie is uiteraard een heel belangrijke partner hierin. Dat betekent dat ENISA, het Europees cybersecurityagentschap, een heel belangrijke rol heeft bij het ondersteunen van de lidstaten bij de desbetreffende strategieën in hun beleid. Dat ENISA niet met naam en toenaam in de strategie staat, wil dus niet zeggen dat het daar geen onderdeel van uitmaakt of dat het kabinet daar geen oog voor heeft. Het agentschap speelt bijvoorbeeld een heel belangrijke rol bij het uitrollen van de certificeringsschema's onder de Cybersecurity Act. Daarnaast werken we heel nauw samen met ENISA in bijvoorbeeld de NIB-samenwerkingsgroep. Daarin wordt op Europees niveau samengewerkt op het gebied van de implementatie van de NIB. Ik probeer de afkortingen te vermijden. Dat proberen we met z'n allen. Daardoor wordt de spreektijd iets langer. Maar dat is dus de implementatie van de netwerk- en informatiebeveiligingsrichtlijn.
Volt vroeg of ik niet te veel rekening houd met veiligheid en bijvoorbeeld te weinig met gebruiksgemak. Informatieveiligheid, en veiligheid sowieso, is altijd onderwerp van afweging. Daarbij worden allerlei belangen tegen elkaar afgewogen. De balans tussen het bieden van weerstand tegen dreigingen en het gebruiksgemak hoort daar gewoon bij. Die afweging moet je dus altijd maken. Die belangenafweging krijgt ook altijd aandacht, onder meer door het voeren van debatten met de Kamer natuurlijk, maar ook door gesprekken die we met verschillende organisaties hebben gevoerd. Het is dus absoluut een terugkerend thema.
Mevrouw Koekkoek van Volt vroeg ook waar de balans tussen privacy en veiligheid ligt. Ik geloof dat ze in haar inbreng de woorden «tegengestelde belangen» gebruikte. Ik probeer heel erg die belangen niet tegengesteld te laten zijn, want dat betekent dat je de een altijd belangrijker vindt dan de ander, terwijl we die balans juist met elkaar proberen te bewaken in een wereld die heel snel verandert en waarin dreigingen reëel zijn. Dat betekent dat je dus altijd weer moet kijken naar die balans en in dit geval naar de digitale weerbaarheid. Bij het inzetten van bevoegdheden, bijvoorbeeld omwille van de onlineveiligheid, internationale veiligheid of nationale veiligheid, maken we altijd een zorgvuldige afweging tussen de collectieve veiligheid en individuele grondrechten en publieke waarden. Volgens mij is het belangrijk dat we altijd kunnen uitleggen waarom een bepaald voorstel op deze manier gebalanceerd is.

Dan de monitoringsvraag van Volt. Mevrouw Koekkoek vroeg of de Kamer in het begin van het jaar een brief kan krijgen over de manier waarop over de voortgang kan worden gerapporteerd. Eigenlijk heb ik deze vraag al aan mevrouw Dekker-Abdulaziz beantwoord. We zullen ervoor zorgen dat we de Kamer elk jaar goed informeren. Het actieplan kan ook bijgesteld worden als er nieuwe ontwikkelingen zijn. De jaarlijkse monitoring van het plan vindt nu dus volgend jaar richting kerst plaats, maar vooruitlopend daarop zullen we u voor de zomer een brief sturen over de voortgang van de integratie van de verschillende organisaties.
Dan de PVV. Dat ging over het zijn van coördinerend bewindspersoon en de regie op de uitvoering. Coördinerend Minister zijn op een onderwerp is niet nieuw. In die zin is het dus niet zo heel creatief. Dat komt gewoon vaker voor. In dit geval, in het geval van de Nederlandse cybersecuritystrategie, kan die alleen maar succesvol ten uitvoer worden gebracht in een nauwe samenwerking tussen bedrijfsleven, wetenschap, decentrale, regionale en nationale overheden, uitvoeringsorganisaties en overigens ook al mijn collega's in het kabinet. Want allemaal hebben zij de verantwoordelijkheid bij te dragen aan stevige cybersecuritymaatregelen. Ik heb de vraag van mevrouw Van Weerdenburg niet zo gehoord dat zij wil dat ik al die verantwoordelijkheden naar mij toe trek. Wil zij dat? Nee, ik kan me niet voorstellen dat ze dat van mij wil. Het is op zich interessant om daar een keer verder over te praten, over alleenheerschappij, maar dat was niet helemaal hoe we dit hadden ingericht. De vraag hoe je daar vervolgens op gaat sturen, is natuurlijk wel een reële vraag. Want het is mooi als je het op papier zet, maar iedereen moet wel zijn ding doen. Dat betekent dat ik bijvoorbeeld ook heel concreet andere Ministers, andere bewindspersonen, zal aanspreken op de voortgang. Dat komt ook bij elkaar, of dat nou in de ministerraad is, in een onderraad of in de monitoringsstukken. Op het moment dat wij zien dat zaken anders lopen of anders moeten, zullen wij daar ook echt werk van maken. Dan zullen wij daarop wijzen en als dat nodig is, zullen wij daarbij ook ondersteunen. En als het nodig is om dat op een andere manier te doen, zullen we daar op een andere manier op sturen. Ik zal er ook voor zorgen dat dit in de monitoring terugkomt. Neem de waterschappen, waar ik het zojuist over had. Neem je het zo specifiek en wil je daar dan een plan bij hebben zodat dat goed is geregeld, dan moet dat wel onder de verantwoordelijkheid van de desbetreffende Minister gebeuren. Maar wij zullen daarbij dan wel kritisch meekijken en daar ook op sturen. Eigenlijk doen we het altijd zo bij onderwerpen die onder een coördinerend bewindspersoon vallen.
Ik heb er nog maar een paar.
Volt sprak nog over de snelle implementatie van de ...

De **voorzitter**:
Voor u vervolgt, is er nog een interruptie van mevrouw Van Weerdenburg, PVV.

Mevrouw **Van Weerdenburg** (PVV):
Voorzitter, ik moest heel even wachten om te zien of dat blokje inderdaad...
Oké. De Minister van Justitie en Veiligheid zit hier dus niet als woordvoerder van de hele groep die erover gaat. Ze is wel echt de chef tegenover wie de rest moet verantwoorden wat eraf is of waarom het niet af is. Ik ben nog heel even op zoek om welk hoofd de Kamer dan moet vragen, want dat vind ik wel een probleem. Bij CSIRT staan bijvoorbeeld twee ministeries. Wie gaat nou over CSIRT? Ik maak mij echt zorgen over de wendbaarheid. Als het anders moet, wie bepaalt dat dan? Wie kan zeggen: er komt een ijsberg ... Op deze manier klinkt het alsof er 30 kapiteins op één schip staan. Wie neemt het besluit om bij te sturen als er een ijsberg opdoemt? Of gaat dit echt eerst langs vier overlegtafels?

Minister **Yeşilgöz-Zegerius**:
Ik snap het. Neem CSIRT. Daarvoor ben ik eindverantwoordelijk, maar er zijn wel verschillende opdrachtgevers. Dan zal het dus afhangen van de vraag die op dat moment concreet speelt. Mevrouw Van Weerdenburg kan altijd als eerste bij mij terecht. Op het moment dat ik denk dat het echt een inhoudelijke verantwoordelijkheid van een vakminister betreft, zal ik niet zeggen: dat kunnen wij niet met elkaar afspreken; u moet daar zijn en ik hoor wel of dat gelukt is. Want zo werkt Den Haag ook weleens. Dan zullen wij er ook ambtelijk extra alert op zijn dat dat wel goed komt, zodat Kamerleden vervolgens wel gewoon antwoord krijgen. Want daar gaat het om. Ik denk dat het mevrouw Van Weerdenburg verder een zorg zal zijn van wie zij dat antwoord krijgt, als ze maar ziet dat er verantwoordelijkheid wordt genomen en iemand antwoord geeft. Dat we daar wel op die manier naar kijken, is ook een taak voor het coördinerende ministerie. Stel nou dat er sprake is van een crisis. U weet dat we een andere crisisstructuur hebben. Dan vervalt al het voorgaande en dan kom je in de crisisstructuur terecht. Maar ook dan hangt het er weer van af wat voor crisis het is en wat er aan de hand is. Begin volgend jaar zullen we ook een integraal sturingsmodel voor de Nederlandse cybersecuritystrategie inrichten. Daarbij zal er expliciet aandacht zijn voor deze samenwerking.

De **voorzitter**:
Dank u wel. Vervolgt u uw betoog.

Minister **Yeşilgöz-Zegerius**:
Dan was er dus nog een vraag van Volt over de snellere implementatie van acties. Volgens mij heb ik daar tegenover andere leden al uitvoerig op gereageerd.
Als ik mij niet vergis, heb ik alleen nog van de VVD een vraag over. Die gaat over het wettelijk mogelijk maken van al die elementen. Ik had al aangegeven dat het wettelijk borgen, het juridisch borgen, nog weleens tijd kan kosten. Mevrouw Rajkowski vraagt of ik dan wel snel ga starten. Mede dankzij de snelle acties van de Kamer is per 1 december de Wet beveiliging netwerk- en informatiesystemen in werking getreden. Daarnaast wordt op dit moment gewerkt aan de implementatie van de NIB2-richtlijn. Ook het grote belang van cybersecurity maakt het echt noodzakelijk dat de richtlijn zowel tijdig als zorgvuldig wordt geïmplementeerd. Dat pakken we dus voortvarend op. Overigens verwacht ik dat dit zal leiden tot een grondige wijziging van de Wet beveiliging netwerk- en informatiesystemen eind 2024. Maar we zitten daar dus middenin. De implementatietijd neem ik daarin ook op. Tevens verwacht ik dat onder meer de integratie van die verschillende organisaties en de oprichting van het publiek-privaat samenwerkingsplatform ervoor gaan zorgen dat een aanvullende wijziging van het huidige wettelijke kader nodig is. Dat zijn we op dit moment aan het onderzoeken. We bekijken ook wat er nog meer nodig is. Ik denk dat ik samenvattend tegen mevrouw Rajkowski kan zeggen dat we op geen enkele wijze denken: nou, die wetgeving komt wel. Daar zitten we echt bovenop. Op het moment dat we ergens versnelling nodig hebben zal ik dat, zoals ik dat eerder heb gedaan, aan de Kamer kenbaar maken met een onderbouwing waaruit blijkt waarom die versnelling daar nodig is. We zullen daarbij dus gebruikmaken van het aanbod dat naar mijn mening in deze commissie bestaat van gewoon tempo: alles wat je sneller kan doen, moet je sneller doen; kom maar naar de Kamer en dan kijken we of het sneller kan.

Mevrouw **Van Weerdenburg** (PVV):
Kan de Minister nog één keertje heel helder aangeven waar de nieuwe strategie nou meer gestroomlijnd is dan de oude situatie met, zeg maar, de lappendeken en honderdduizend clubjes? Eerlijk gezegd, had de PVV verwacht dat we nu een soort stroomschema zouden hebben, zo van: die,

die en die wil die. Wij hadden verwacht dat het een soort afgeslankte, effectievere vorm zou zijn. Ik heb het gevoel dat al die clubjes, al die instanties en al die organisaties er nog steeds zijn en dat er gewoon meer lijntjes getrokken zijn. Dan ben je niet sneller, wendbaarder en flexibeler in een tijd van crisis. Kan de Minister nog één keer aanwijzen waarin die flexibiliteit dan wel zit?

Minister **Yeşilgöz-Zegerius**:
Misschien twee dingen. Wat doen we hier echt anders? Aan de cybersecuritystrategie is nu echt een actieplan toegevoegd. Dat is anders dan de voorgaande keren. Wat ook echt anders is, is dat we die organisaties gaan samenvoegen. Dat zal echt tot minder van die lijntjes leiden. Wat we kunnen doen, is in ieder geval een poging wagen om bij de monitoring – binnen een jaar verneemt u de stand van zaken – inzichtelijker te maken hoe die stroomlijning eruitziet. Ik begrijp wel waar mevrouw Van Weerdenburg naar zoekt: dat steeds meer bij elkaar brengen, dat veel meer bundelen. Zo is het actieplan in ieder geval wel opgezet. Nogmaals, hoe die stroomlijning eruitziet op het moment dat er een crisis is, kunnen we ook heel duidelijk aangeven. Misschien kunnen we dat voor de zomer voor een ander debat nog eens inzichtelijk maken. Maar ik zou deze wel mee willen nemen in de monitoring om elk jaar nog scherper te maken hoe dat eruitziet. Bijvoorbeeld het samenvoegen van die organisaties en het feit dat er een concreet actieplan ligt, zijn twee heel concrete zaken waardoor er veel meer focus is of, in dit geval, zal zijn.

De **voorzitter**:
Ik bedank de Minister voor de beantwoording. Ik kijk even naar de leden. Is er behoefte aan een tweede termijn? Ik zie geknik. Dan zou ik willen voorstellen om daar meteen mee aan te vangen.
Ik geef het woord aan mevrouw Rajkowski van de VVD.

Mevrouw **Rajkowski** (VVD):
Dank, voorzitter. Ik zeg ook dank voor de informatie en de beantwoording van onze vragen. Die worden zeer gewaardeerd en zijn ook verhelderend. We wachten even op het herziene plan waar het kabinet mee komt. Daar kijken we zeker naar uit. Als ik in de plannen uit 2020 met ctrl-f zoek op «analoog», krijg ik één hit. Zoek ik op «terugvaloptie», dan krijg ik er ook één. Beide komen voor in de inleiding, namelijk bij de constatering dat het risico steeds groter wordt. Wij wachten de plannen dus even af, maar ik ga ervan uit dat die dan ook terugkomen in de paragraaf met oplossingen en dat soort dingen. In ieder geval dank daarvoor.
Ten tweede heb ik toch nog een vraag over het oefenen. De Minister begon over ISIDOOR. Dat is, denk ik, een zeer gewaardeerde grootschalige oefening. Daar is de VVD zeker echt blij mee, maar bij ISIDOOR wordt alleen digitaal geoefend. Het effect van wat er nou op straat gebeurt, wordt niet meegenomen. Misschien zou dat dan nog een mooie zijn: wat gebeurt er nou in de fysieke wereld als het digitaal fout gaat? Wellicht bij de voorbereiding op de volgende ISIDOOR-oefening. Dat zou misschien een mooie toevoeging zijn aan de oefening van volgend jaar. Graag een reactie.

De **voorzitter**:
Dank u wel. Dan is nu het woord aan mevrouw Van Weerdenburg, PVV.

Mevrouw **Van Weerdenburg** (PVV):
Voorzitter. Ik wil niet de spelbreker zijn. We zijn hartstikke blij dat dit stuk er nu ligt. We hebben er alleen lang op moeten wachten, zullen we maar zeggen. De niet-malse kritiek, ook van de Cyber Security Raad, ligt er al heel erg lang.

Ik ga het maar gewoon zeggen: ik vind echt wel dat dit meer handen en voeten had moeten hebben. Daar had ik op gehoopt. Ik meen ook dat de Minister ons dat wel in het vooruitzicht had gesteld. We hebben het heel vaak over een organogram gehad. Maar nu hoor ik: de monitoring komt nog, en een sturingsmodel. Misschien kan de Minister nog iets uitgebreider zeggen wat dat sturingsmodel dan precies is. Want dat klinkt een beetje als de sneeuwbal die ons al eerder is beloofd en die ik had verwacht in dit stuk. Het is dus nog lang niet af. Dat vindt zowel de PVV als BVNL teleurstellend, ook gezien het feit dat het veld en alle organisaties schreeuwen om snelheid, snelheid, snelheid. Ik wil hier wel gezegd hebben dat dit allemaal te langzaam gaat. We moeten misschien juist daarom nadenken over een iets afgeslanktere vorm van de hele crisisstructuur, want er zijn nu nog heel erg veel spelers, veel te veel kapiteins op ons schip. Ondanks het feit dat we blij zijn met de toezegging van de Minister dat er niets zal doorschuiven naar een andere Minister – dat hebben we aan tafel bij deze commissie eerder weleens letterlijk gezien, dus daar ben ik blij mee – denk ik alsnog dat het een voordeel zou zijn als er iets minder mensen aan de overlegtafels zouden zitten. Dat zouden we liever hebben.
Ik hoop dat het allemaal sneller kan. Ook de stukken die hier nog ontbreken, heb ik liever eerder dan pas over een jaar, want dan zitten we alweer bijna aan het einde van de zittingsperiode van deze Kamer. Als het sneller kan: heel graag!
Ik hoor liefst nog even van de Minister wat er specifiek in het sturingsmodel staat. Wat is precies de monitoring? Is het dan volledig?

De **voorzitter**:
Dank u wel, mevrouw Van Weerdenburg. Dan is het woord aan mevrouw Dekker-Abdulaziz van D66.

Mevrouw **Dekker-Abdulaziz** (D66):
Voorzitter, dank u wel. Dank aan de Minister dat ze in ieder geval onze oproep «hoe sneller, hoe beter» heeft meegekregen. Dat was een duidelijke oproep en zij pakt die op.
De Minister heeft voor het eind van het jaar een brief toegezegd waarin gekeken zal worden naar de plannen en de acties en wanneer die komen. Ik neem aan dat in die brief ook per actie staat wanneer die gaat komen en welke acties er zijn. Het liefst moet dit inderdaad niet aan het eind van het jaar zijn, maar eerder. Kan de Minister dat toezeggen?
Verder dank voor de antwoorden over de gemeenten. D66 zal zich blijven inzetten voor het behouden van encryptie.
Dank u wel.

De **voorzitter**:
Dank u wel, mevrouw Dekker-Abdulaziz. Ik kijk naar de Minister. Zij heeft vijf minuten nodig. Ik schors voor vijf minuten en daarna gaan we door met de beantwoording.

De vergadering wordt van 11.39 uur tot 11.41 uur geschorst.

De **voorzitter**:
Ik kijk naar de Minister voor de beantwoording van de resterende vragen. De Minister.

Minister **Yeşilgöz-Zegerius**:
Dank u wel. Ik heb alle onderstrepingen, oproepen/vriendelijke waarschuwingen gehoord. Ik ga direct naar de vragen. Mevrouw Rajkowski van de VVD vroeg: kan bij de volgende ISIDOOR-oefening ook meegenomen worden wat in de fysieke wereld gebeurt? Het fysieke aspect wordt deels meegenomen. Dat zal de volgende keer dus ook zo zijn. De vorige keer

vielen in de oefening bijvoorbeeld de matrixborden op de snelwegen uit. Dat is dan een combi. Maar hoe relevant het is, hangt ook van de partner en de deelnemende organisatie af. Dat is zeker een aspect.
Mevrouw Van Weerdenburg vroeg naar het organogram en het sturingsmodel. Het sturingsmodel bestaat straks grofweg uit twee delen, namelijk publiek en privaat. We gaan met de private sector in gesprek over wat door hen wordt opgeleverd, hoe het eruit gaat zien en hoe we dat met elkaar kunnen monitoren. Tegelijkertijd is er een stuurgroep met verschillende departementen, zodat iedereen daar aan tafel zit. We zullen met monitoring inzichtelijk maken hoe het ervoor staat. Nee, ik haal het door elkaar. Dat betreft de vraag van mevrouw Dekker-Abdulaziz. We zullen hier begin volgend jaar ook over rapporteren. Ik zal kijken of ik óf daarbij óf bij wat u voor de zomer van ons krijgt over de samenvoeging al een hele stap kan maken rond het organogram, waar mevrouw Van Weerdenburg naar op zoek is.
Misschien nog iets over crisis. Op het moment dat er een crisis is, gaan we in de MCCb-structuur zitten. Dat hebben we afgelopen jaar ook meegemaakt, bijvoorbeeld met de oorlog in Oekraïne, waarbij je zag dat veel Oekraïense vluchtelingen hiernaartoe kwamen. We hebben het ook meegemaakt met corona. Er zijn verschillende momenten geweest. Denk ook aan de asielcrisis in de zomer. Dan kom je in een andere structuur. De Minister van Justitie en Veiligheid of de Minister-President is dan voorzitter van zo'n crisisoverleg. Alle relevante partners zitten daar op zo'n moment, vooral vanuit de departementen, aan tafel. Je kan dan heel snel besluiten nemen. Op het moment dat de piek van de crisis voorbij is, ga je die ook weer afschakelen. Dat is omdat je alles weer zo veel mogelijk in reguliere besluitvormingsprocessen wil hebben, zodat bijvoorbeeld de Kamer dat kan volgen.
Dan het laatste punt, van mevrouw Dekker-Abdulaziz over de monitoring. De mensen thuis en hier zouden gehoord kunnen hebben «voor het einde van dit jaar», maar het is volgend jaar. We gaan 'm nu namelijk pas vaststellen, dus je kunt over een jaar gaan monitoren wat er gedaan is in dat jaar. De planning van de actielijnen is dan al ingenomen, maar we zullen één keer per jaar zo inzichtelijk mogelijk maken hoe het allemaal bij elkaar komt, dus een totaalbeeld schetsen, waar ook mevrouw Van Weerdenburg naar op zoek is.
Even kijken of ik daarmee alles heb gehad. Volgens mij heb ik én alles goed gezegd én geen toezeggingen gedaan waar de mensen die ermee aan de slag moeten, totaal van in paniek raken.

De **voorzitter**:
Ik kijk heel even rond. Ik zie dat er geen aanvullende vragen zijn. Dank u wel, Minister. Dan rest mij nog wel om even de toezeggingen op te lezen. Ik heb mijn bril op; dat scheelt. Graag even aandacht van eenieder, met de vraag of we dit goed genoteerd hebben. De twee eerste toezeggingen zijn eigenlijk geen nieuwe toezeggingen, maar omdat ze wel een paar keer aan de orde kwamen in dit debat, vind ik het toch goed om ze even te benoemen. De eerste toezegging betreft een toezegging naar aanleiding van een discussie met mevrouw Rajkowski.

– De Minister stuurt het geüpdatete nationaal crisisplan digitaal voor het einde van het jaar naar de Kamer; er werd zelfs gezegd «voor het kerstreces».

Dan een toezegging aan de gehele commissie, die ook al stond maar die toch nog gememoreerd is.

– Jaarlijks informeert de Minister de Kamer over de voortgang van de Nederlandse Cybersecuritystrategie. Hierbij zal de Minister ook de structuur van het cybersecuritystelsel inzichtelijk maken. Zo mogelijk zal de Minister dat al eerder met de Kamer delen.

Dat is het punt over het organogram naar aanleiding van de discussie met mevrouw Van Weerdenburg.

– De Minister informeert de Kamer begin volgend jaar over het sturingsmodel op cybersecurity.

O, dat hangt samen.

Minister **Yeşilgöz-Zegerius**:
Ja, dat is wel Q1. Dat is een van de actielijnen. Die hebben allemaal hun eigen planning. Aan het einde van het jaar brengen we het steeds bij elkaar. Het sturingsmodel is dus Q1. De monitoring is over een jaar.

De **voorzitter**:
Dan vullen we bij die laatste nog Q1 in.
Daarmee zijn we aan het einde gekomen van dit commissiedebat. Ik dank uiteraard de Minister en de ambtenaren, ook de ambtenaren die niet in deze zaal maar achter de schermen zitten, en zeker ook degenen die bijgedragen hebben aan het stuk. Ik laat 'm nog een keer zien, Minister. Dat is altijd goed. Ik zie een aantal mensen op de publieke tribune zitten die eraan meegewerkt hebben. Ik dank uiteraard de leden en de mensen thuis, maar zeker ook de mensen op de publieke tribune. Dank u wel.

Sluiting 11.46 uur.