9
Cybersecurity vitale waterwerken

Aan de orde is het **debat** over **het rapport van de Algemene Rekenkamer over cybersecurity van vitale waterwerken**.

De **voorzitter**:
We gaan nu een debat voeren over het rapport van de Algemene Rekenkamer over cybersecurity van vitale waterwerken. Voor de duidelijkheid merk ik op dat daaronder worden verstaan: waterkeringen onder beheer van Rijkswaterstaat die door de minister zijn aangewezen als vitale onderdelen binnen de sector Keren en beheren van water.

Voordat ik de eerste woordvoerder de gelegenheid geef om zijn tekst uit te spreken, merk ik nog het volgende op. Dit debat betreft het rapport van de Algemene Rekenkamer over cybersecurity en vitale waterwerken. Er is een vertrouwelijke bijlage bij het rapport ter inzage gelegd in de Kamer en er heeft een vertrouwelijke briefing plaatsgevonden. Voor de leden van de Kamer geldt dat zij niet mogen citeren uit de aangeboden stukken of uit de briefing. Als dit wel gebeurt, kan het Presidium in de gelegenheid worden gesteld om te bepalen of er sprake is van schending van de vertrouwelijkheid en om de eventuele consequenties te bepalen. Het zal niet nodig zijn om die bepalingen toe te passen, maar het is mijn plicht u dit te zeggen.

Dan zijn we op het punt gekomen dat het debat een aanvang kan nemen. De spreektijd is voor elke fractie vier minuten. Ik zal twee interrupties per fractie toestaan. Ik geef als eerste het woord aan de heer Von Martels van het CDA.

De heer **Von Martels** (CDA):
Voorzitter, dank u wel. Ik had eigenlijk zeven minuten aangevraagd, maar heb vier minuten gekregen. Ik zal dus wat sneller moeten gaan praten.

Voorzitter. Wij, de bewoners van de delta van Rijn en Maas aan de Noordzee, worstelen al sinds mensenheugenis met het water dat ons omringt. Met terpen, dijken, molens en polders hebben we een haat-liefdeverhouding met water. Vaak konden we het water wel de baas zijn, maar soms niet, zoals in 1953. Maar door indrukwekkende civiele werken, zoals de Deltawerken, hebben we wereldfaam gekregen en lijkt het alsof we het water voor eens en voor altijd de baas blijven.

Het keren van het water is als vitale sector aangemerkt. Dat is logisch, want miljoenen mensen zijn voor hun veiligheid afhankelijk van de betrouwbaarheid van de waterwerken. Ook de economische belangen zijn groot. Decennialang lag de nadruk op hardware, asfalt, beton, sluizen, dijken en waterkeringen, maar de laatste twee decennia treedt ook de digitale revolutie in de vitale waterwerken in. Dat levert grote voordelen op, maar maakt ons afhankelijk. We moeten cyberdreigingen onder ogen zien. Spionage, sabotage, terrorisme en criminaliteit kunnen zich verplaatsen naar de digitale wereld en bedreigen dan ook de automatisering van waterwerken. Het is goed dat de Algemene Rekenkamer hierover een rapport heeft uitgebracht. In haar onderzoek heeft ze gekeken naar de wijze waarop vitale waterwerken beschermd zijn tegen cyberaanvallen. Na het lezen van het rapport was ik niet echt gerustgesteld. Integendeel, we moeten ook het signaal van de AIVD in zijn laatste jaarverslag serieus nemen. Daar zegt de AIVD in toenemende mate activiteiten te signaleren die erop zijn gericht digitale sabotage van vitale infrastructuur in Europa mogelijk te maken. Rijkswaterstaat schiet op een aantal fronten tekort. Zo is de strategie van detectie en respons nog niet voltooid. Het SOC, het Security Operations Center van Rijkswaterstaat, had de ambitie om eind 2017 bij alle vitale waterwerken cyberaanvallen direct te kunnen detecteren, maar in het najaar van 2018 was dat nog niet gerealiseerd. Dat klinkt heel zakelijk. Als ik dat concreet maak met een voorbeeld, gaat het misschien leven, maar dan overtreed ik de aan mij opgelegde geheimhouding. Het in het rapport van de Algemene Rekenkamer genoemde object Alfa en de werkwijze zouden al genoeg moeten zijn om alle alarmbellen te doen afgaan.

Rijkswaterstaat schiet ook tekort op het gebied van crisisdocumentatie. Die is verouderd en voor een door een cyberaanval veroorzaakte crisis blijkt geen specifiek scenario te bestaan. De Algemene Rekenkamer ziet dat belangrijke documenten bij de bestrijding van een cyberaanval op onderdelen niet actueel worden gehouden en dat er geen pentesten worden gehouden. Organisaties laten zich in die zogenoemde pentesten bewust hacken door een ingehuurde partij om informatie te verkrijgen over kwetsbaarheden in hun beveiligingssysteem. Waarom voert Rijkswaterstaat nauwelijks pentesten voor vitale waterwerken uit?

Ook de tunnelveiligheid speelt hier een rol. Voor de veiligheid in tunnels heeft onze fractie vaak aandacht gevraagd. Steeds was het antwoord dat we ons geen zorgen hoefden te maken en dat het wel goed zat met die tunnelveiligheid. Na het lezen van het rapport van de Algemene Rekenkamer vraag ik me af of die geruststelling juist was. Zijn onze tunnels, juist vanwege de mogelijke cyberaanvallen, wel veilig?

De Algemene Rekenkamer komt met een achttal aanbevelingen en de minister antwoordt de Algemene Rekenkamer dat ze alle aanbevelingen overneemt. Het CDA is daar voor nu tevreden mee. Het is duidelijk dat de minister de gesignaleerde problemen serieus neemt. Toch willen we nog de volgende accenten leggen. Veel aanbevelingen gaan over het spoedig afronden van maatregelen die al eerder getroffen hadden moeten zijn, bijvoorbeeld het aansluiten van de vitale waterwerken op het SOC. Dit had eind 2017 al gerealiseerd moeten zijn. Waarom is dat niet gebeurd? Wanneer is dat wel gedaan? De Algemene Rekenkamer beveelt de minister ook aan om het actuele dreigingsniveau te onderzoeken en te besluiten of extra mensen en middelen nodig zijn. Daarom mijn vraag: heeft de minister extra mensen of middelen nodig? Zijn de middelen toereikend of wordt er nog met MS-DOS gewerkt? De Algemene Rekenkamer vindt het voor een snelle en adequate reactie op een crisissituatie ook van essentieel belang dat de noodzakelijke informatie up-to-date is. Pentesten zouden integraal onderdeel uit moeten maken van de cybersecuritymaatregelen bij vitale waterwerken. Wat is de stand van zaken? Is de informatie nu up-to-date? Worden er nu pentesten gehouden? Verder zou volgens de Algemene Rekenkamer moeten worden bezien of medewerkers van het SOC beter moeten worden gescreend. Gebeurt dat nu? Dan het vijfde punt. Voorzitter, ik zie dat ik door mijn tijd

ben, maar het is fijn dat u mij nog even deze laatste regels laat uitspreken.

De **voorzitter**:
Ja. Doe maar.

De heer **Von Martels** (CDA):
De Algemene Rekenkamer noemt ook de cascade-effecten. Dat zijn effecten die een crisis in een vitale sector kan hebben op andere vitale sectoren, zoals vervoer of energie. Rijkswaterstaat heeft dat niet goed in beeld. Met de waterschappen is wel een samenwerkingsovereenkomst gesloten om tijdig te kunnen reageren op incidenten die grote cascade-effecten kunnen hebben. Zijn de cascade-effecten nu goed in beeld? En zo nee, wanneer is dat dan wel op orde?

Voorzitter. Ik ben benieuwd naar de beantwoording door de minister.

Mevrouw **Van Brenk** (50PLUS):
Ik hoor de heer Von Martels van het CDA zeggen dat de minister alle aanbevelingen overneemt. En toch zie ik dat de manier waarop zij reageert neerkomt op "ik ga eerst nog onderzoeken en dan eens verder kijken". En dit terwijl het in 2017 had moeten gebeuren. U zei het zelf al. Toen had het geregeld moeten zijn en toen hadden al die vitale onderdelen bij dat center aangesloten moeten zijn. En dat is niet gebeurd. Waarom zegt u dan dat de minister het doet en dat u tevreden bent?

De heer **Von Martels** (CDA):
Mevrouw Van Brenk stipt wel iets aan waarover ik het volledig met haar eens ben. Natuurlijk hadden die zaken allang gerealiseerd moeten worden, maar we zitten nu met de situatie van vandaag. Dat betekent dat de minister nu moet gaan handelen op wat de Rekenkamer naar voren heeft gebracht. De minister heeft bij haar aantreden duidelijk gezegd dat zij vindt dat er een rapport over moet komen. Dat is een compliment aan deze minister; zij heeft dit onderzoek in ieder geval zelf geïnitieerd. Maar vervolgens zal een duidelijk antwoord gegeven moeten worden op de aanbevelingen van de Rekenkamer.

Mevrouw **Van Brenk** (50PLUS):
Is de heer Von Martels het met ons eens dat het antwoord van de minister niet kan zijn "ik ga nog verder onderzoeken", maar dat er nu daadkracht getoond moet worden, dat er gehandeld moet worden, dat dit ook gerealiseerd moet worden en dat we niet nog in 2020 eens kunnen kijken of het nou wel gerealiseerd is?

De heer **Von Martels** (CDA):
Zeker, er moet daadkracht getoond worden, maar er zal misschien toch eerst even onderzoek gedaan moeten worden zodat blijkt wat de verstandigste wijze is om dat te realiseren en die daadkracht te tonen.

De heer **Van Aalst** (PVV):
We weten allemaal dat er een gigantische opgave ligt voor het onderhoud, ook wat betreft de cybersecurity. Is het CDA bereid om daar geld voor vrij te maken?

De heer **Von Martels** (CDA):
Er zal heel welbewust gekeken moeten worden waar de prioriteiten nu moeten komen te liggen. Als je het rapport zo leest, dan denk je haast wel dat er iets moet gaan gebeuren, ook in financiële zin, maar ik ben wel eerst benieuwd naar de beantwoording van de minister daaromtrent. In dit rapport staat wel het nodige waarvan je zou kunnen vermoeden dat het niet zomaar kan gebeuren zonder dat je daar extra middelen voor vrijmaakt.

De heer **Van Aalst** (PVV):
We hebben natuurlijk vanochtend nog gesproken met de Rekenkamer. Het is gewoon heel duidelijk: zonder extra budget gaan we het gewoon niet redden. Gaat het CDA vanuit dat oogpunt bezien dan ook gewoon budget vrijmaken?

De heer **Von Martels** (CDA):
We zullen zien welke besluiten het CDA daarover gaat nemen. We wachten eerst de beantwoording van de minister daarover af.

De **voorzitter**:
Dan is nu het woord aan mevrouw Van Brenk van 50PLUS.

Mevrouw **Van Brenk** (50PLUS):
Dank, voorzitter. Al bij haar aantreden heeft de minister aangegeven werk te willen maken van cybersecurity op haar beleidsterreinen. Dat is een streven waar 50PLUS achter staat. Op het gebied van waterwerken werd het programma BWR, Beveiligd Werken Rijkswaterstaat, opgestart en grotendeels doorlopen. Prima. Tot zover de complimenten.

De Algemene Rekenkamer heeft geconstateerd dat de strategie van detectie en respons weliswaar is ingericht, maar nog niet is voltooid. Het Security Operations Center, het SOC, is hiertoe ingericht, maar de ambitie om eind 2017 bij alle vitale waterwerken cyberaanvallen direct te kunnen detecteren was in het najaar van 2018 nog niet gerealiseerd. Rijkswaterstaat zou een cyberaanval op een vitaal waterwerk dus pas kunnen bespeuren als het te laat is. En dat is op z'n zachtst gezegd zorgwekkend, zeker in het licht van de constatering dat sommige regio's terughoudend zijn bij het nemen van extra maatregelen. Waarom zijn zij terughoudend, vraag ik de minister, en wat doet u daartegen? Daarnaast geeft het SOC aan over te weinig kennis en capaciteit te beschikken. Dat lijkt mij ondenkbaar en onwenselijk, zeker gezien het feit dat bij een onderzocht vitaal waterwerk nog geen maatregelen ter detectie van een cyberaanval zijn getroffen.

De pentesten, de penetratietesten, werden net al genoemd. Ook die worden lang niet altijd uitgevoerd. Dus nogmaals concreet de vraag: wat doet u hieraan?

Een andere belangrijke vraag is waarom die genoemde ambitie, die al in 2017 gehaald had moeten zijn, eind 2018 nog niet was gehaald. Hoe staat het daar nu mee? Een aantal waterwerken die Rijkswaterstaat beheert, zijn vitaal. Een aanval op de IT van deze waterwerken kan grote gevolgen hebben voor Nederland. Het kan zelfs een kwestie van leven of dood worden. Daarom is het noodzakelijk dat alle vitale waterwerken rechtstreeks zijn aangesloten op het Security Operations Center van Rijkswaterstaat. Die ambitie om vanaf eind 2017 cyberaanvallen op al die vitale waterwerken direct te kunnen detecteren, was in het najaar van 2018 nog niet gerealiseerd. Hierdoor bestaat, zeg ik nogmaals, het risico dat Rijkswaterstaat te laat reageert. Nogmaals, hoever zijn we op dit moment? Is dat op dit moment nog steeds het geval? Dat de financiering niet geregeld is, kan wat ons betreft geen argument zijn, want dat geld had er immers in 2017 al moeten zijn. Kan de minister aan ons bevestigen dat geld daadwerkelijk geen probleem mag zijn en kan ze garanderen dat dit ook niet zo is?

De minister maakt de uitvoering van de aanbevelingen van de Rekenkamer afhankelijk van het resultaat van het onderzoek naar het dreigingsbeeld. Wat 50PLUS betreft: no way! Dat kan echt niet. Aansluiting op SOC is hoe dan ook noodzakelijk, want nogmaals, dit had al in 2017 moeten gebeuren. Nu moet er boter bij de vis komen. Wij willen een toezegging van de minister dat dit ook gaat gebeuren. Want als we met zijn allen de cybersecurity van vitale waterwerken zo cruciaal vinden, en dat vinden we, moeten we alles in het werk stellen om het geheel zo snel mogelijk veilig te krijgen. Bedreigingen moet je immers niet alleen bestrijden, het is net zo belangrijk dat je die bedreigingen voorkomt. Dat is het doel van een sluitende cybersecurity. Graag een reactie van de minister hierop.

Al met al blijft 50PLUS toch zitten met een ongemakkelijk gevoel. Datzelfde gevoel hebben wij ook bij achterstallig onderhoud aan wegen en bruggen. Daar gaan we binnenkort over praten. We rekenen op niet mis te verstane antwoorden en een doortastend optreden van deze minister.

Dank, voorzitter.

De **voorzitter**:
Dank, mevrouw Van Brenk.

□

De heer **Remco Dijkstra** (VVD):
Voorzitter. De Algemene Rekenkamer publiceerde een rapport over de cybersecurity van onze waterwerken. U heeft precies gezegd wat dit inhoudt: de tunnels, de dijken, de sluizen en de waterkeringen in ons land, die ons beschermen tegen het water. We weten allemaal wat dit kan betekenen. Veel van die waterwerken zijn uitgerust met automatiseringssystemen uit de jaren negentig. In de loop van de jaren zijn deze gekoppeld aan netwerken om het uitlezen en bedienen op afstand mogelijk te maken, maar daardoor is natuurlijk wel de kwetsbaarheid toegenomen. Via een hack zou je als IT'er schade kunnen aanrichten.

De VVD wil dat de ICT bij de vitale waterwerken op orde is. Natuurlijk is alles te kraken als je kwaad wilt, maar het gaat erom dat we zelf niet de controle verliezen. Het gaat overigens niet alleen om de hardware of de software, maar ook om de mindware, de cultuur, en om de vraag hoe je omgaat met je personeel. Is je personeel gescreend? Dat zou natuurlijk de zwakste schakel kunnen zijn in het hele ketenverhaal. Graag een reactie van de minister op de screening van mensen. De VVD en ook Nederland willen denk ik gerustgesteld kunnen worden.

Het belang van onze veiligheid staat voorop. Wat ons betreft is er voldoende regelgeving. De instrumenten zijn er ook. Het komt dus aan op de uitvoering. Ben je er klaar voor als iemand kwaad wil? We moeten voorkomen dat iemand inbreekt in de digitale omgeving en daarmee het functioneren van de vitale waterwerken kan beïnvloeden, met alle gevaren van dien.

Het is ook belangrijk om te constateren dat de minister bij haar aantreden zelf een aantal waterwerken als vitaal heeft aangemerkt. Ze is er dus zelf mee begonnen, ook omdat ze volgens mij inziet wat het kan betekenen. Er is ook al heel veel: een brief herziening Strategie Nationale Veiligheid, de herijking vitale infrastructuur en de verbetering crisisbeheersing 2015, een Besluit en wet meldplicht cybersecurity 2017, het Besluit beveiliging netwerk- en informatiesystemen, voorschriften, EU-richtlijnen, een Wetboek van Strafvordering over computercriminaliteit en natuurlijk recent de Wet op de inlichtingen- en veiligheidsdiensten. Dat zijn allemaal zaken waarvoor ook de VVD zich heeft ingezet. Die moeten ervoor zorgen dat de overheid de nationale veiligheid als kerntaak kan zien en kan waarborgen.

Hoewel we juridisch nu dus zijn opgewassen tegen de dreiging en tegen de moderne communicatiemiddelen, zijn we er nog niet, want als slechts 60% is uitgevoerd door Rijkswaterstaat, is er beslist nog werk te doen om het noodzakelijke beschermingsniveau te krijgen. Dan is het niet voldoende om alleen alle aanbevelingen van de Rekenkamer over te nemen. Dat is te makkelijk. Als we het signaal van de Rekenkamer serieus willen nemen, moeten we ook ieder jaar inzicht krijgen in de voortgang. Daar zou de minister ons over moeten informeren. De VVD wil dus dat de minister doorgaat met het verbeteren van de automatisering en de beveiliging van onze waterwerken. Ik wil graag zelf weten wat er nodig is aan tijd, geld of mankracht om de veiligheid van onze waterinfrastructuur beter te beschermen tegen cyberterroristen of mensen die simpelweg kwaad in de zin hebben. De gevolgen kunnen immers groot zijn.

Ik vraag me af in hoeverre we iedere keer zelf het wiel uitvinden. Kunnen we leren, zeker als het gaat om cybersecurity, van andere departementen waar dit soort zaken ook spelen? Doet Rijkswaterstaat dit project alleen, of is die samenwerking relevant? Of het nu is bij Defensie, bij ICT-projecten, bij telecom, bij JenV: overal en op ieder niveau is er een aanpak om cybermisbruik tegen te gaan. Zou de kennis daarover overkoepelend delen binnen de overheid kunnen helpen? Hoe kijkt de minister daartegen aan?

Het kabinet heeft in het regeerakkoord 95 miljoen beschikbaar gemaakt. In welke mate kan Rijkswaterstaat of het ministerie van Infrastructuur en Waterstaat daaruit putten?

Onze belangrijkste digitale systemen en netwerken moeten gewoon goed worden beveiligd. We mogen criminelen niet de kans geven om Nederland plat te leggen met een cyberaanval. De minister moet daarbij goed aangeven wat ze nodig heeft. Dan wil de VVD haar daarbij helpen.

Dank u wel.

De **voorzitter**:
Dank, meneer Dijkstra. Ik geef de heer Stoffer van de SGP het woord.

☐

De heer **Stoffer** (SGP):
Voorzitter. Stelt u zich eens het volgende voor. Het is 2030 en het 5G-netwerk is uitgerold door een Chinees staatsbedrijf. Alle waterkeringen zijn aangesloten op dit netwerk. Ondertussen is er een noordwesterstorm op komst, die aanzwelt tot orkaankracht. Nederland rekent uiteraard op zijn ICT. Ondertussen is China uit op het aanpakken van Europese landen. Er wordt een cyberaanval uitgevoerd op een van de keringen. Nederland zou in paniek zijn. U begrijpt dat we het zover gewoon niet laten komen. Aan de voorkant niet, door het inperken van Chinese inmenging bij de uitrol van onze digitale netwerken, maar ook aan de achterkant niet, door ervoor te zorgen dat onze ICT-systemen op orde zijn, zeker bij kwetsbare objecten als waterkeringen.

Ik wil de minister vanaf hier een compliment maken. Zoals 50PLUS daarnet ook aangaf, is ze gelijk bij haar aantreden aan de slag gegaan met dit vraagstuk. Ik denk dat ze verheugd is dat de Algemene Rekenkamer hier kritisch naar gekeken heeft. De Rekenkamer geeft aan dat Rijkswaterstaat de afgelopen jaren veel heeft gedaan, maar dat er nog meer moet gebeuren omdat het nog niet op orde is. Door de Rekenkamer ingeschakelde hackers wisten bij een bepaald object het ICT-systeem binnen te dringen. Het is van belang dat de minister zorgt voor een voortvarende uitvoering van alle aanbevelingen die in het rapport staan. Ik schat in dat het een retorische vraag is, maar: gaat ze dat ook doen?

Voorzitter. Ik heb nog drie specifieke punten. De minister wil de opvolging van de aanbevelingen afhankelijk maken van uit het onderzoek verkregen dreigingsbeelden. De Rekenkamer geeft echter de waarschuwing af dat een deel van die aanbevelingen maatregelen betreffen die al eerder genomen hadden moeten worden. Met andere woorden, ga aan de slag en wacht niet op die dreigingsbeelden. Ik ben benieuwd hoe de minister hier tegen aankijkt.

De Rekenkamer geeft ook aan dat het cruciaal is om zogenaamde pentesten te doen, dus bewust laten hacken om te zien waar die kwetsbaarheden zitten. Maar ik lees dat Rijkswaterstaat hier niet aan wil, omdat het te riskant zou zijn. Ik ben erg benieuwd waarom dat te riskant is en waarom dat niet gewoon gedaan wordt. Ik zou zeggen: dat heb je toch juist nodig om je kwetsbaarheden bloot te leggen?

Als laatste en het is al eerder aangehaald: er is geen apart budget meer voor het programma Beveiligd Werken Rijkswaterstaat en dat terwijl we zien dat er nog stevige slagen te maken zijn. Dat zorgt in de praktijk voor vertraging en uitstelgedrag. Hoe gaat de minister dat voorkomen? Want geld mag niet het probleem zijn. In aansluiting op wat de vorige spreker, de heer Dijkstra zei, zeg ik: laat de minister gewoon aangeven wat nodig is en dan zullen we ervoor moeten zorgen dat dat budget daarbij komt.

Voorzitter, tot zover. Dank u wel.

De **voorzitter**:
Dank, meneer Stoffer. Meneer Schonis van D66, het is tijd voor uw inbreng.

☐

De heer **Schonis** (D66):
Dank u, voorzitter. Ik begin met opmerkelijk nieuws. Gisteren is een laptop verkocht voor 1,1 miljoen euro. Op die laptop staan de zes meest gevaarlijke computervirussen, zoals ILOVEYOU, Mydoom en WannaCry. Wereldwijd hebben deze virussen gezorgd voor meer dan 85 miljard dollar aan schade. De kunstenaar Guo O Dong heeft van de laptop een kunstwerk gemaakt om aandacht te vragen voor de risico's van digitalisering in onze maatschappij.

Voorzitter. Van het kunstwerk van Guo O Dong is het maar een kleine stap naar de cybersecurity van onze eigen natte kunstwerken. Als Zeeuw ligt de veiligheid van waterstaatswerken mij uiteraard nauw aan het hart. Het doemscenario dat de heer Stoffer net schetste, is natuurlijk wel iets waar je als Zeeuw rekening mee houdt. Het onderwerp van Guo O Dong waar hij aandacht voor vraagt, is een hartstikke belangrijk onderwerp bij onze vitale natte infrastructuur. Ik ben dan ook blij met het grondige onderzoek van de Rekenkamer en de aanbevelingen die zijn gepresenteerd. De conclusie dat de digitale veiligheid nog niet op orde is, moeten we serieus nemen. De minister ziet het onderzoek als ondersteuning van het door haar ingezette beleid, maar wat ons betreft mag daar nog wel een stapje bij.

Zo constateert de Rekenkamer dat niet bij alle vitale kunstwerken een cyberaanval geconstateerd kan worden. Wat doet de minister met die conclusie en welke maatregelen gaat zij op korte termijn nemen? Is zij bereid vitale waterwerken voorlopig niet op het internet aan te sluiten om risico's van aanvallen op die manier te verkleinen?

Maar ook op andere aanbevelingen uit het onderzoek verwacht D66 dat de minister snel actie gaat ondernemen. Zo beveelt de Rekenkamer aan onderzoek te doen naar het actuele dreigingsniveau van een cyberaanval op de vitale waterwerken. Dat moet snel gebeuren want de minister wil het programma Beveiligd Werken Rijkswaterstaat, het BWR, snel afronden. Is de minister bereid dit onderzoek voor het eind van het zomerreces te doen en kan er dan nog in het najaar worden gewerkt aan de resterende maatregelen uit dat BWR-programma?

Dan de aanbevelingen van de Rekenkamer over het aanscherpen van het screeningsniveau van de medewerkers van het Security Operations Center, het SOC. Kan de minister toezeggen ook hierover voor het einde van het zomerreces met concrete maatregelen te komen? Ook dit had in 2017 al gebeurd moeten zijn.

Tot slot, de pentesten oftewel de botsproeven. Wat D66 betreft zijn pentesten een belangrijk onderdeel van cybersecurity. Rijkswaterstaat zegt echter dat pentesten voor bepaalde kunstwerken risicovol zouden zijn. De Rekenkamer doet aanbevelingen om deze risico's expliciet te maken. Uiteindelijk moet de pentest een integraal onderdeel zijn van de cybersecurity van alle kunstwerken. Is de minister dat met ons eens? Ik lees dat de minister de mogelijkheid van pentesten gaat onderzoeken. Wanneer kunnen we de resultaten daarvan tegemoetzien?

Voorzitter, ik rond af. Bij de Oosterscheldekering is in het beton het gedicht van Ed Leeflang gebeiteld. Dat eenregelige gedicht luidt als volgt: "Hier gaan over het tij, de maan de wind en wij". Ik hoop toch niet dat wij deze mooie dichtregel zouden moeten vervangen door: "Wie gaat er eigenlijk over het tij, de maan een hacker of wij?".

Dank u wel, voorzitter.

De **voorzitter**:
Dank u wel, meneer Schonis. Mevrouw Kröger van GroenLinks.

Mevrouw **Kröger** (GroenLinks):
Voorzitter. De Rekenkamer onderzocht de cyberveiligheid van onze waterwerken en constateert een groot aantal verschillende problemen, die ook niet allemaal altijd met elkaar samenhangen. Eigenlijk hoor ik heel veel dezelfde zorgen vanuit de verschillende leden van onze commissie.

Het zit deels in techniek en het zit deels in bestuurlijke afspraken, maar om te beginnen is het ook nog niet eens duidelijk wat nou het risico is en hoe groot dat is. Dat maakt het natuurlijk extra lastig om ons daartegen te verweren. De minister gaf aan dat ze werkt aan een digitale cyberstrategie. Daaruit moet duidelijk worden of, waar en wanneer er dreigingen zijn. Daarbij moet de opmerking geplaatst worden dat dreigingen steeds veranderen en vernieuwen. Dat is natuurlijk onderdeel van de risico's. We moeten ons dus wapenen tegen een aanval die we nog niet zelf hadden kunnen bedenken.

Voor dit dossier moet dat betekenen dat kwaadwillenden de netwerken niet binnen kunnen dringen door afgeschermde netwerken, beveiligde computers, protocollen en goed toezicht. Dat geldt tegenwoordig natuurlijk eigenlijk voor elke overheidsdienst en voor elk bedrijf, maar zeker voor onze waterwerken. Het werkbezoek van vorige week aan Rijkswaterstaat maakte dat nogmaals heel duidelijk. Hoe krijgen we nou veel beter zicht op de risico's, zo vraag ik de minister.

De Rekenkamer constateert, en dat punt werd ook eerder gemaakt, dat veel van de automatiseringssystemen stammen uit de jaren tachtig en negentig. Rijkswaterstaat geeft aan zich niet te willen gaan richten op modernere systemen, maar op detectie en response. Maar moeten we die oude computersystemen niet sowieso moderniseren? En als er geen geld is en er geen plannen zijn om die systemen te gaan vervangen, is dat dan niet reden voor een heel apart debat?

Dan met betrekking tot detectie en response. De vraag is inderdaad: is er voldoende capaciteit bij het SOC? Voorziet de minister dat we hier stevig in moeten investeren? Dat is wederom een geldvraag.

Voorzitter. Dat fysieke infrastructuur vernieuwen en moderniseren geld en tijd kost, snap ik heel erg goed. Maar de Rekenkamer constateert ook dat het uitvoeren van maatregelen en het afdwingen van inspecties niet bij alle regio's worden afgedwongen. Welke mogelijkheden ziet de minister om dit probleem op te lossen, en om Rijkswaterstaat en SOC meer in positie te brengen?

De Rekenkamer constateert verder: de doelen zijn niet behaald, de uitvoering is niet voltooid, de documentatie blijkt verouderd en de onderhoudscontracten staan beveiliging in de weg. Het is een heel scala aan pittige kwalificaties, die je eigenlijk in geen enkele doorlichting zou willen zien of lezen. Ik ben heel benieuwd naar de reactie van de minister hierop.

Dan nog een vraag: in hoeverre zijn die vitale waterwerken standalone? Dus in hoeverre is het zo dat een noodaggregaat niet werkt zonder de autorisatie van een computer 200 kilometer verderop? Kan de minister ons geruststellen dat de belangrijkste installaties ook autonoom hun belangrijkste functies kunnen vervullen?

Ten slotte. Er zijn in andere commissies vaker gesprekken geweest en vragen gesteld over of en welke buitenlandse bedrijven mogen meedingen bij aanbestedingen voor gevoelige contracten en vitale infrastructuur, bijvoorbeeld als het gaat om ons 5G-netwerk. Hoe zit dit bij de beveiliging van onze waterwerken? Hoe zorgen we dat we niet door WTO-regels gedwongen worden om de besturing van onze waterwerken in vreemde handen te geven?

Dank u wel, voorzitter.

De **voorzitter**:
Dank, mevrouw Kröger. Dan krijgen we meneer Drost van de ChristenUnie.

De heer **Drost** (ChristenUnie):
Dank u wel, voorzitter. Je moet er toch niet aan denken dat bijvoorbeeld de Maeslantkering vanwege een vliegende storm met springtij moet sluiten, maar dat deze vanwege een cyberaanval openblijft. De maatschappelijke ontwrichting en de economische schade zouden immens kunnen zijn. Met dit in gedachten heb ik mijn bijdrage van vanmiddag voorbereid.

Gelukkig is in Nederland alles erop gericht om een volgende watersnoodramp te voorkomen. Nadat de overheid in de twintigste eeuw steeds reageerde op een ramp, na de Zuiderzeeramp in 1916, de watersnoodramp in 1953 en de bijna-ramp in het rivierengebied in 1993 en 1995, ging ongeveer tien jaar geleden het roer om, en werd met de start van het Deltaprogramma expliciet het doel om met de investeringen in waterveiligheid een volgende ramp voor te blijven. Het is een mooie benadering die uniek is in de wereld. Het is een verstandige benadering. En het is natuurlijk een logische benadering, met een kwart van ons land dat onder de zeespiegel ligt en bijna 60% dat overstroombaar is. Om die bescherming handen en voeten te geven, hebben we een uitgekiend stelsel van dammen, duinen, dijken en waterkeringen. Die waterkeringen hebben beweegbare onderdelen, die met behulp van gedigitaliseerde processen worden bediend. Daar komt de cybersecurity om de hoek kijken. Cyberaanvallen zijn een relatief nieuwe bedreiging waar we ons tegen moeten wapenen, juist bij deze vitale fysieke infrastructuur, die essentieel is voor het veilig voortbestaan van ons land. Voordat ik daar verder op inga, zeg ik de Algemene Rekenkamer dank voor zijn onderzoek naar de wijze waarop vitale waterwerken beschermd zijn tegen cyberaanvallen. De Rekenkamer bedoelt daarmee bewuste pogingen om schade te veroor-

zaken. Om je daartegen te beschermen, is er cybersecurity. Dat is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen, en als die toch is ontstaan, te herstellen. Doordat processen sterk zijn gedigitaliseerd, is vitale infrastructuur, waaronder waterwerken, kwetsbaarder dan ooit voor cyberaanvallen. Dit onderzoek en de aanbevelingen zijn daarmee zeer relevant.

Voorzitter. De conclusies en aanbevelingen zijn helder en goed, van cascade-effecten tot betere screening van personeel. De minister zegt toe alle aanbevelingen over te nemen. Ze zegt daarbij dat veel van de aanbevelingen afhankelijk zijn van opvolging van de eerste aanbeveling inzake het duiden van het dreigingsniveau. In de reactie daarop wijst de Rekenkamer er fijntjes op dat een aantal van zijn aanbevelingen gaat om het spoedig afronden van maatregelen die al eerder getroffen hadden moeten zijn. Ze doelen daarmee bijvoorbeeld op het aansluiten van die vitale waterwerken op het SOC, het Security Operations Center, zodat meer diepgaand en actueel zicht is op deze waterwerken. Dit had al eind 2017 gerealiseerd moeten zijn en is dus niet afhankelijk van de eerste aanbeveling. Kortom, de Rekenkamer vindt dat de minister zich net te veel verschuilt achter het voldoen aan de eerste aanbeveling. Mijn vraag is dan: hoe reageert de minister hierop? Wat is de actuele stand in het wegwerken van dit soort achterstallige actiepunten? En wat kan de minister zeggen over de allocatie van eventueel extra benodigde middelen hiervoor, bijvoorbeeld voor de doorontwikkeling van het SOC?

Voorzitter. Voor het goede begrip: tijdens bijvoorbeeld het werkbezoek vorige week maandag aan Rijkswaterstaat ben ik onder de indruk geraakt van hoe actief zij werken aan het beveiligen van vitale infrastructuur en digitale processen tegen cyberaanvallen. Ook is duidelijk dat er tot op heden geen echte ongelukken met cyberaanvallen zijn geweest. De vraag blijft of wat we doen, genoeg is in deze tijd van toenemende cyberdreiging. Hoe kijkt de minister hiertegen aan? Is de samenwerking tussen Rijkswaterstaat en waterschappen enerzijds en veiligheidsdiensten en dergelijke anderzijds wel intensief en effectief genoeg? Deze vraag bedoel ik niet alleen vanuit RWS-zijde van het spectrum, maar juist ook vanuit de veiligheidsdiensten zelf. Hoe proactief wordt RWS gewaarschuwd door bijvoorbeeld AIVD of MIVD met betrekking tot eventuele cyberaanvallen vanuit een of andere trollenfabriek of buitenlandse mogendheid?

Voorzitter. Tot slot kom ik terug bij het voorbeeld waarmee ik begon, de Maeslantkering. Ik heb specifiek een vraag over de faalkans. Daar is altijd veel over te doen en dat is logisch, aangezien de faalkans het daadwerkelijke beschermingsniveau beïnvloedt. Het bekendste voorbeeld van een discussie over de faalkans is die van de Maeslantkering. In het ontwerp van deze wonderschone kering is uitgegaan van een faalkans van 1 op 1.000. In de praktijk ligt deze echter veel hoger. Een aantal jaar geleden werd er zelfs gesproken over 1 op 100. Mijn vraag in dit debat is: in hoeverre werkt het risico op cyberaanvallen al of niet door in de faalkans van waterwerken in het algemeen en van de Maeslantkering in het bijzonder?

Dank u wel, voorzitter. Wij zien uit naar de beantwoording van onze vragen.

De **voorzitter**:
Dank, meneer Drost. Tot slot in deze termijn is het woord aan de heer Van Aalst van de PVV.

☐

De heer **Van Aalst** (PVV):
Dank u wel, voorzitter. De conclusies die de Algemene Rekenkamer trekt over hoe het met de cybersecurity van onze vitale waterwerken staat, zijn snoeihard. Bij de uitvoering van het programma Beveiligd Werken Rijkswaterstaat is het niet gelukt om alle gestelde doelen te behalen, de inrichting van het Security Operations Centre is nog niet voltooid, belangrijke documentatie van Rijkwaterstaat om zich tegen aanvallen te kunnen weren, is verouderd en tot slot test Rijkswaterstaat de maatregelen die ze tegen aanvallen hebben, nauwelijks met pentesten. Het is geen mooie opsomming, al helemaal niet als we beseffen wat er op het spel staat. Want als de cybersecurity faalt, staat de veiligheid van ons land op het spel. Als de waterwerken worden aangevallen en door derden bestuurd kunnen worden, is de schade niet te overzien. Het is een gevaar dat wij ons in onze strijd tegen het water niet kunnen permitteren.

De minister stelt dat het wegnemen van risico's door de systemen te moderniseren volgens Rijkswaterstaat technisch uitdagend en kostbaar is. Rijkswaterstaat richt zich daarom met name op de signalering van een cyberaanval en een snelle reactie om die aanval onschadelijk te maken. Op beide gebieden moet Rijkswaterstaat nog stappen zetten om aan de eigen doelstellingen voor cybersecurity te voldoen. De PVV is hier ernstig over verontrust. De boel is, kort gezegd, gewoon niet op orde. De minister moet keihard aan het werk gaan om te voorkomen dat Al Qaida straks onze waterwerken kan hacken. De PVV stelt daarom de volgende slotvraag: wanneer is de veiligheid wel op orde en hoe garandeert de minister dat in deze tussenperiode de veiligheid van Nederland niet op het spel staat?

Dank u wel.

De **voorzitter**:
Dank, meneer Van Aalst. Daarmee zijn we gekomen aan het einde van de eerste termijn van de Kamer. Ik schors de vergadering tot 16.00 uur. Dan gaan we luisteren naar de beantwoording door de minister.

De vergadering wordt van 15.47 uur tot 16.00 uur geschorst.

De **voorzitter**:
We gaan verder met het debat over het rapport van de Algemene Rekenkamer over cybersecurity van vitale waterwerken. Ik geef het woord aan de minister van Infrastructuur en Waterstaat.

☐

Minister **Van Nieuwenhuizen-Wijbenga**:
Dank u wel. voorzitter. We hebben vanmiddag een heel belangwekkend onderwerp met elkaar te bespreken. Ik ben blij dat de Kamerleden zich er allemaal zo serieus in verdiept hebben, want het gaat niet voor niets om de vitale belangen van ons land.

Ik wil beginnen met de Algemene Rekenkamer dank te zeggen voor het gedegen onderzoek dat ze hebben gedaan. Een aantal Kamerleden memoreerde dat ook al. Ik heb vanaf het begin van mijn aantreden zelf ook cybersecurity uitdrukkelijk als aandachtspunt gekozen. Dat had er natuurlijk ook mee te maken dat ik me op mijn vorige plek in het Europees Parlement ook veel met digitalisering en cybersecurity heb beziggehouden. Ik heb ook in Europees verband, waar ENISA de club is die dat voor Europa in de gaten houdt, kunnen constateren hoe kwetsbaar we met z'n allen zijn. Als je dan, zoals in mijn geval, verantwoordelijk bent voor de vitale infrastructuur, dan is dat een nieuwe dreiging die je heel erg serieus moet nemen. Ik heb in mijn kennismakingsgesprekken bij de Algemene Rekenkamer met de heer Visser en met mevrouw Giskes, die hierover gaat, uitdrukkelijk dit onderwerp naar voren gebracht. Ik heb gezegd: als mij als minister gevraagd zou worden wat ik zelf belangwekkend vind om te onderzoeken, dan is dat dit onderwerp. Ik ben dus heel blij dat ze dat hebben gedaan. Ik vind het ook heel erg nuttig. En ik was er natuurlijk ook wel op voorbereid dat het niet allemaal al honderd procent op orde zou zijn.

Ik heb al eerder gezegd, en ook in reactie op het onderzoek, dat ik het echt zie als een ondersteuning van beleid. Maar ik zie wel degelijk de scherpte van de aanbevelingen, dat er dus ook echt werk aan de winkel is. Ik wil me er voortvarend voor inzetten om die aanbevelingen zo snel mogelijk over te nemen.

De indruk bestaat dat we mogelijk met die aanbevelingen zouden wachten, dat we eigenlijk alles uitstellen totdat we eerst dat actuele dreigingsbeeld voor elkaar hebben. Dat is, denk ik, wat onhandig en cryptisch opgeschreven in de brief, want dat is absoluut niet de bedoeling. Ik wil uiteraard direct aan de slag met de aanbevelingen. U hebt als Kamer helemaal gelijk, waar het gaat om zaken die eigenlijk in 2017 al op orde hadden moeten zijn en waar dat nu nog steeds niet het geval is, dat u zegt: dan gaat de minister toch niet zitten wachten tot er een nieuw dreigingsbeeld klaar is. Dat gaan we dus ook niet doen. We gaan gewoon voortvarend aan de slag met alle aanbevelingen. Ik zal daar verderop in de beantwoording per aanbeveling graag op terugkomen.

De heer **Remco Dijkstra** (VVD):
We hadden laatst ook weer zo'n sessie met de Algemene Rekenkamer. Dan zei de heer Visser, de president van die Rekenkamer: het makkelijkste wat bewindspersonen doen, is het overnemen van de aanbevelingen. En daarmee is het eigenlijk van tafel. Dat willen we niet. We willen dat ze op tafel liggen. We willen dat helder is wat de aanbevelingen zijn en wat we in feite per aanbeveling gaan doen. We willen dat u daar ook over terugkoppelt naar de Kamer. Die wens hebben wij volgens mij allemaal uitgesproken, omdat die urgentie inderdaad gevoeld wordt, niet alleen intrinsiek door u maar ook door ons, omdat het belangrijk is voor ons land. We moeten niet alleen zeggen: bedankt voor het rapport. Dat moet zeker niet het geval zijn.

Minister **Van Nieuwenhuizen-Wijbenga**:
Dat gevoel deel ik helemaal. Ik had het later in de beantwoording willen doen, maar ik kan het net zo goed nu zeggen: ik bewillig graag in het verzoek van de heer Dijkstra om hier jaarlijks over te rapporteren. Ik stel me voor dat we dat voor het eerst in de aanloop naar de begroting zullen doen, zodat we dat kunnen meenemen in die jaarlijkse cyclus. Dat zal dan echt wel wat uitgebreider zijn dan dat we alleen opmerken dat we er voortvarend mee aan de slag zijn. Dan ga ik echt wel in op die aanbevelingen.

Ik wil nog iets zeggen over het actuele dreigingsbeeld. Mevrouw Kröger maakte er een heel terechte opmerking over toen ze zei dat dat natuurlijk nooit af is. Dreigingen veranderen voortdurend op globaal niveau. Dus we zullen daar een eerste aanvang mee moeten nemen en dat voortdurend moeten blijven testen. Verschillende Kamerleden hebben ook opmerkingen gemaakt over de afstemming met de AIVD, de MIVD en de collega-ministeries. Dat zullen we in dat verband dus ook blijven doen en daarin samen ook optrekken. Maar het eerste specifieke dreigingsbeeld dat we nu met elkaar gaan maken, wil ik benutten om te kijken of dit nu voldoende is. De heer Dijkstra maakte terecht ook net een punt: als een minister zegt "alle aanbevelingen overnemen", dan is het netjes binnen de lijntjes kleuren en dan is de kous af. Nee, dan ben ik zelf ook echt ambitieuzer en wil ik, afhankelijk van wat er uit het dreigingsbeeld komt, ook kijken of we nog meer moeten doen, of we echt daarbovenop nog iets moeten doen. Uw vraag was ook: hebben we nu voldoende in huis, is er voldoende budget, om de om de aanbevelingen uit te kunnen voeren? Voor de huidige aanbevelingen is dat het geval. Dat kúnnen we doen, maar ik wil wel aan de hand van het dreigingsbeeld kijken of dit ook onvoldoende is, of dat er misschien toch nog meer nodig is. Daar wil ik dat echt voor gebruiken, en het ook steeds tegen het licht blijven houden of we er dan mee zijn.

De screening. Natuurlijk zit de kwetsbaarheid — ik vond dat de heer Dijkstra daar wel een mooie voor had — niet alleen in de hardware en de software, maar ook in de mindware. Als je de verkeerde mensen op de verkeerde plek hebt, dan kun je alles qua hardware en software mooi voor elkaar hebben, maar dan ben je nog steeds ontzettend kwetsbaar. Dus voor het menselijke aspect, eigenlijk de zwakste schakel in die hele beveiliging — dat blijkt overal keer op keer — hebben we ook echt aandacht. Dat richt zich aan de ene kant natuurlijk op het vergroten van het bewustzijn van mensen die dit werk doen zodat ze niet, soms toch onbewust, risicovolle situaties creëren. En anderzijds is het natuurlijk echt erop gericht dat mensen niet bewust met kwaadwillende partijen gemene zaak maken.

Al een aantal jaren moeten beheerders en bedieners van op afstand bedienbare objecten bij RWS ook verplicht een awarenesstraining volgen. En daarnaast zijn er trainingen en awarenessprogramma's voor managers en bestuurders van RWS. Binnen IenW zijn we overigens ook bezig met een breed awarenessprogramma. Ik onderschrijf zeker de aanbeveling van de Algemene Rekenkamer dat het natuurlijk hiernaast van belang is dat medewerkers die in aanraking komen met die gevoelige systeeminformatie van onze vitale objecten op het juiste niveau gescreend zijn. Ik vond het ook echt een tekortkoming waar ik, zeg ik maar heel open, zelf ook van schrok. Het is meteen voortvarend opgepakt om daaraan te werken, dus dat loopt nu, dat project is opgestart om die medewerkers allemaal wel op het goeie niveau te screenen. Dat zal natuurlijk nog wel een aantal maanden vragen, maar ik ga ervan uit dat we dat voor het eind van het jaar allemaal op orde hebben. Dus RWS is hard aan het werk om alle medewerkers van het SOC naar dat hogere screeningsniveau te brengen.

We moeten straks dan ook nog weer kijken, afhankelijk van dat dreigingsniveau, daar laat ik dat dan wel even van afhangen, of we dat ook nog moeten doortrekken naar andere doelgroepen. Ik laat dus zorgvuldig kijken naar het ophogen van beveiligingsniveaus van objecten en het eventueel nog voorschrijven van een hogere screeningsniveau voor meerdere mensen binnen de organisatie.

Een ander punt dat door velen van u is opgemerkt, zijn de pentesten, de zogenaamde penetratietesten en de oefenprogramma's. Natuurlijk is het uitvoeren van allerlei testen noodzakelijk, om meerdere redenen. Allereerst natuurlijk gewoon om te kijken of de objecten wel functioneren zoals ze moeten functioneren, of de geplande noodmaatregelen werken en efficiënt zijn, of de benodigde verbetermaatregelen dan daadwerkelijk wel zijn doorgevoerd en het gewenste effect opleveren, et cetera. Daarvoor heeft Rijkswaterstaat een uitgebreid testinstrumentarium. Dat varieert van heel eenvoudig uit te voeren testen met nauwelijks impact op het gewone werk tot hele complexe en kostbare testen. Een voorbeeld van die laatste categorie, die echt wat verdergaat, is de zogenaamde penetratietest. Ook bij de keuze welke specifieke test wanneer waarvoor wordt ingezet, werkt Rijkswaterstaat risicogestuurd. Er wordt een afweging gemaakt tussen het risico van niet voldoende testen en de kosten die zijn gemoeid met de keuze voor een specifieke test en de consequenties die die testen kunnen hebben voor de continuïteit van het object of het systeem dat wordt getest. Maar natuurlijk is dit rapport van de Algemene Rekenkamer wel degelijk een spiegel hiervoor geweest. Dus de afweging om die penetratietest te doen zal nog nadrukkelijker in beeld komen. Er wordt zeker meer van de mogelijkheid daartoe gebruikgemaakt.

In het regeerakkoord is structureel 95 miljoen vrijgemaakt voor cybersecurity. Een deel daarvan is inderdaad bestemd voor de sectoren waarvoor mijn ministerie verantwoordelijkheid draagt. Het gaat om een bedrag van 4 miljoen in 2019, 6 miljoen in 2020 en vanaf 2021 om een bedrag van 7 miljoen euro. Dat is het onderdeel dat wij daarvan hebben gekregen.

De heer Dijkstra vroeg in hoeverre de overheid telkens hetzelfde wiel opnieuw uitvindt. Wordt het nou niet breder opgepakt? Doet Rijkswaterstaat dit alleen? Wat doe je met andere partners? Er wordt gelukkig heel veel samengewerkt op het terrein van cybersecurity, onder leiding van collega Grapperhaus. Dat is binnen het Rijk. Maar ook tussen het Rijk en andere partijen gebeurt dit. Meteen bij de start van deze periode heb ik breed aandacht gevraagd voor cybersecurity. Ik roep het addendum in herinnering dat inmiddels is toegevoegd aan het Bestuursakkoord Water. Want ook voor de waterschappen is dit natuurlijk ontzettend belangrijk: niet op het niveau van de vitale keringen, maar wel op hun niveau. Het gaat dan meer om economische schade. Ik ben ook heel erg blij dat we nu met het addendum cybersecurity bij het Bestuursakkoord Water ook volop de inzet van alle waterschappen hebben om hier serieus een verbeterslag in te maken.

De heer **Von Martels** (CDA):
Ik hoor de minister zeggen dat er breed wordt samengewerkt binnen het kabinet om cybersecurity aan te pakken, maar het is de verantwoordelijkheid van de minister van JenV. Mijn vraag aan deze minister is: in hoeverre heeft zij daarover veelvuldig contact met minister Grapperhaus en hoe is die kabinetsbrede aanpak? Hoe kunt u die het best formuleren?

Minister **Van Nieuwenhuizen-Wijbenga**:
De kabinetsbrede aanpak zelf valt onder verantwoordelijkheid van collega Grapperhaus, maar we hebben natuurlijk heel regelmatig contact hierover in de diverse onderraden die wij hebben op de dinsdag. Daar bespreken we deze onderwerpen met alle betrokken ministers. Dat geldt ook voor cybersecurity. Dan zit ik daar dus vanuit de IenW-kant aan tafel. Als het wat meer gedetailleerd is, schuift ook de dg Rijkswaterstaat daarbij aan. Dus wij hebben daar regelmatig overleg over.

De heer **Von Martels** (CDA):
Het gaat mij er natuurlijk met name om die cascade-effecten te voorkomen. De andere vitale sectoren zijn ook ontzettend kwetsbaar. Het is dus weliswaar de verantwoordelijkheid van de minister van JenV, maar ik kan me niet voorstellen dat deze minister daar heel nauw bij betrokken is.

Minister **Van Nieuwenhuizen-Wijbenga**:
Ik denk dat de heer Von Martels helemaal gelijk heeft. Wij kijken in gezamenlijkheid naar die cascade-effecten. Inderdaad, collega Grapperhaus is coördinerend voor cybersecurity en de vitale infrastructuur, maar J en V heeft ook al een onderzoek uitgevoerd naar cascade-effecten en er wordt nu ook onderzocht welke maatregelen daarvoor noodzakelijk zijn. Vanwege de concurrentiegevoeligheid daarvan worden de uitkomsten alleen gedeeld met de vitale aanbieders, zoals ze heten. Dus dit onderzoek pakken wij natuurlijk ook op voor ons onderdeel, maar nogmaals: voor de coördinatie moet ik naar collega Grapperhaus verwijzen.

De heer **Schonis** (D66):
Ik hoorde de minister net een aantal bedragen noemen per jaar, die gereserveerd zijn en al gealloceerd zijn voor de pentesten, tenminste, ik begreep uit uw antwoord dat die pentesten uit die extra bedragen betaald gaan worden. Maar als je die pentesten vaker doet, komen natuurlijk nieuwe zaken naar voren en moet je daar weer extra geld voor reserveren. Ik zou toch een wat meer planmatig antwoord van de minister willen over hoe ze dit in de komende jaren structureel gaat verbeteren.

Minister **Van Nieuwenhuizen-Wijbenga**:
De bedragen die ik net noemde, waren gerelateerd aan het stukje dat mijn ministerie heeft gekregen uit die 95 miljoen die speciaal voor cybersecurity in het regeerakkoord werden genoemd. Dus dat is niet het totaalbedrag. Dat waren de bedragen die jaarlijks vanuit dat bedrag voor IenW beschikbaar zijn. Maar wij hebben natuurlijk binnen onze eigen begroting ook middelen voor cybersecurity ingezet.

De heer **Schonis** (D66):
Dat is hartstikke mooi om te horen. Mijn vraag was hoe we dan planmatig hiermee omgaan, binnen IenW. Want je hebt nu een keer extra geld gekregen en er is natuurlijk wel eigen geld, maar als je dit op termijn wilt inbedden, kun je er

vergif op innemen dat je daar de komende jaren structureel geld voor vrij moet maken. Gaat u dat planmatig aanpakken?

Minister **Van Nieuwenhuizen-Wijbenga**:
Ja, natuurlijk gaan we dat planmatig aanpakken. Ik gaf u net aan wat we voor de aanbevelingen moeten doen, bijvoorbeeld de aansluitingen op het Security Operations Center (SOC). Daar hebben we nu de middelen voor. Dat gaan we ook doen, maar afhankelijk van wat er uit het dreigingsbeeld komt, gaan we kijken wat er nog meer nodig is en dan zullen we dat inderdaad planmatig aanpakken. Ik heb de heer Dijkstra net toegezegd dat ik de Kamer jaarlijks zal rapporteren hoe het daarmee staat. Ik stel voor dat ik daarin ook de financiële kant van de zaak meeneem.

De **voorzitter**:
Dan vraag ik de minister haar betoog voort te zetten.

Minister **Van Nieuwenhuizen-Wijbenga**:
Ik was nog even bij het onderwerp van de samenwerking. Rijksbreed is er een nationaal detectienetwerk en voor de vitale objecten en ketens brengt het Nationaal Cyber Security Centrum de informatie samen. Dat zorgt er ook voor dat iedereen zijn voordeel kan doen met de informatie die vanuit diverse andere rijksonderdelen wordt gegenereerd. Rijkswaterstaat is ook een van de initiatiefnemers van een joint-SOC voor het Rijk, waar informatie en kennis gedeeld worden. Daar is ook de uitwisseling van personeel middels detachering een invulling van. Ik kan mij nog herinneren dat ik u in het debat over de waterschappen ook heb verteld dat er op roulatiebasis mensen vanuit de waterschappen meelopen op het SOC om zo ook daar die kruisbestuiving tot stand te brengen.

Voor de overheid, voor ketenpartners en ook voor de markt — vergeet niet dat die natuurlijk met dezelfde uitdagingen worstelen — zijn er ook de zogenaamde ISAC's, de Information Sharing and Analysis Centers. Dan gaat het behalve over keren en beheren ook over de havengebieden, over de luchthavens et cetera. Daar zit Rijkswaterstaat ook aan tafel om informatie uit te wisselen en te verrijken, uiteraard in een besloten sessie, omdat het gaat om gevoelige informatie. Daarnaast is er ook nog een rijksbreed directeurenoverleg en een privaat-publiek overleg om maximaal informatie en ideeën te delen.

Over het crisismanagement zijn ook nog vragen gesteld; een heel belangrijk onderdeel van de werkzaamheden van IenW en in het bijzonder van Rijkswaterstaat. Crisisscenario's voor cybersecurityincidenten horen daar logischerwijs bij. Ik heb al vaker met uw Kamer gedeeld dat het natuurlijk altijd gaat om een drieslag. Je moet van tevoren proberen om de preventie op een zo hoog mogelijk niveau te hebben, vervolgens voortdurend monitoren en in de gaten houden wat er gebeurt, omdat zelfs de bedrijven die gespecialiseerd zijn in cybersecurity nooit 100% garantie hebben dat ze niet toch een keer gepenetreerd worden. Dus je moet het voortdurend blijven volgen. Je moet ook altijd voorbereid zijn. Je moet je contingencyplanning op orde hebben, je rampscenario voor als het toch onverhoopt een keer gebeurt, juist omdat je dat nooit voor de volle honderd procent kunt uitsluiten. We moeten die crisisscenario's zeker op orde hebben.

Tijdens het Algemene Rekenkameronderzoek was er al een strategische verkenning gestart om het calamiteitenplan voor cyberincidenten van de juiste scenario's te voorzien. De Rekenkamer heeft gewoon gelijk dat er een specifiek crisisscenario voor cybersecurity moet worden opgenomen. Rijkswaterstaat is conform de aanbeveling al bezig met een actualisatieslag van die crisiskaarten en ook met het proces om te borgen dat we die crisisscenario's actueel houden. Een crisis komt natuurlijk altijd op een onverwacht moment. Het beste wat je kunt doen om toch gesteld te staan, is oefenen, oefenen, oefenen. Interdepartementaal doet mijn ministerie voortdurend mee aan allerlei cybercrisisoefeningen. Dat doen we niet alleen interdepartementaal, maar we gaan dat ook binnen het ministerie doen en ook vaker doen.

In dit kader is ook nog gevraagd naar de buitenlandse bedrijven; ik dacht dat het mevrouw Kröger was. Daarbij volgen we nauwgezet het inkoopbeleid van het ministerie van BZK. Er is vorig jaar vanuit het MCEV gekeken naar een overname van vitale aanbieders. Er is nu ook een uitvraag: hoe ga je ermee om ten aanzien van ICT-componenten? Dat gebeurt allemaal onder leiding van BZK en we volgen nauwgezet de afspraken die daaruit voortvloeien.

Er zijn natuurlijk veel discussies over 5G; u stipte dat heel terecht aan. Bij vitale infrastructuur wil je er natuurlijk niet aan denken dat er dingen mis zouden kunnen gaan. Daar is onder leiding van de NCTV een interdepartementale taskforce voor opgericht. Die taskforce voert een risicoanalyse uit naar de kwetsbaarheden van 5G-telecomnetwerken. Over de uitkomsten hiervan zal uw Kamer geïnformeerd worden door mijn collega van JenV.

De heer Von Martels heeft specifiek een vraag gesteld over de tunnels. De tunnels zijn ook missiekritieke objecten. Die kennen een adequate beveiligingsaanpak. Voor alle factoren, of het nou gaat om de menselijke factor, de fysieke beveiliging, de cybersecurity, de functionele veiligheid, het assetmanagement, al die factoren samen, geldt het pakket van maatregelen op het gebied van preventie, detectie, respons en handhaving. Ook in het kader van de tunnels worden al die dingen bij elkaar gebracht.

Mevrouw Kröger heeft gevraagd: kan de minister ons geruststellen dat de belangrijkste apparaten ook autonoom kunnen blijven opereren? De vitale objecten en apparaten die daarbij horen zijn zo ingericht dat ze ook standalone kunnen opereren. Bij calamiteiten, bijvoorbeeld stroomuitval of een netwerk dat om wat voor reden dan ook platgaat, kan het object nog steeds worden bediend. In veel gevallen gaat het om mechanische varianten en kan er door mensen met de hand iets dichtgedraaid worden en dat soort praktische zaken. Vitale objecten worden ook lokaal bediend. Het is voor ons ontzettend belangrijk om dat te blijven borgen, ook naar de toekomst toe, zodat we nooit helemaal afhankelijk zijn van een digitaal systeem.

Daaraan gekoppeld waren er zorgen over sommige systemen die al heel oud zijn, een beetje een erfenis uit het verleden. Er zijn er inderdaad nog bij die stammen uit de jaren tachtig en negentig. Die systemen zijn nog niet allemaal vervangen, omdat dat een enorme hoge kostenpost met zich meebrengt en soms de continuïteit van het netwerk in

gevaar zou brengen. Dat is meteen ook een antwoord op de vraag over de regio's: waarom waren regio's nou huiverig? Dat had vooral te maken met het feit dat ze bezorgd waren of het middel niet erger zou zijn dan de kwaal, omdat het bewuste object in de tussentijd natuurlijk wel goed moet blijven functioneren. Gelukkig hebben we inmiddels overal die zorgen weg kunnen nemen en hebben alle regio's getekend voor de huidige aanpak.

De heer Drost vraagt hoe proactief Rijkswaterstaat wordt gewaarschuwd door bijvoorbeeld de AIVD over nieuwe dreigingen. Als er signalen zijn of informatie is over mogelijke dreigingen bij de diensten die relevant zijn voor Rijkswaterstaat, wordt dat gelukkig proactief gedeeld. Dat gaat in het geval van Rijkswaterstaat vrijwel altijd via de AIVD.

Ik heb, dacht ik, het merendeel van de vragen beantwoord. Dat hoop ik althans.

De **voorzitter**:
We gaan eens even kijken. Mevrouw Van Brenk.

Mevrouw **Van Brenk** (50PLUS):
Een groot deel van de vragen is inderdaad beantwoord. Ik ben in ieder geval heel blij om te horen dat het budget toereikend is. Geld is geen probleem. Het is fijn om dat eens een keer te horen. Mijn punt was de terughoudendheid van de regio's. De minister zegt daarvan nu dat het is weggenomen: ze hebben allemaal getekend, dus een, twee, drie, vier we gaan ertegenaan! Dan blijft nog steeds staan dat het center zegt onvoldoende kennis en capaciteit te hebben, dus ook capaciteit. De vraag is hoe we dat gaan oplossen en wanneer het, omdat iedereen nu in de startblokken staat, nu helemaal is opgelost.

Minister **Van Nieuwenhuizen-Wijbenga**:
Dat hangt natuurlijk van de aanbeveling af. De ene zal wat eerder klaar zijn dan de andere. We streven ernaar om alles zo veel mogelijk nog in dit jaar opgelost te krijgen. Ik weet niet of dat op alle vlakken zal lukken. Dan uw opmerking over de regio's. Ik ben blij dat ze nu ook aan boord zijn, maar het zal er soms ook van afhangen of je werk met werk kunt maken om iets op een handige manier te doen. Er wordt met man en macht aan gewerkt, ook door de regio's, om het allemaal zo snel mogelijk voor elkaar te krijgen.

Mevrouw **Van Brenk** (50PLUS):
En het stukje over de opleiding en de kennis?

Minister **Van Nieuwenhuizen-Wijbenga**:
Daar kijken we ook nog naar. De huidige aanbevelingen kunnen opgevolgd worden, maar het is sowieso een uitdaging omdat er ook bij Rijkswaterstaat — we hebben dat gisteren bij de ILT ter sprake gehad — een aantal mensen met pensioen gaan. Dat is ook bij Rijkswaterstaat het geval. Niet alleen de mensen die zich met cybersecurity bezighouden, maar in brede zin moeten we voortdurend aandacht blijven houden voor de heel specifieke kennis van deze mensen. Die is ontzettend gewild, veelgevraagd, in de hele samenleving, zowel in de publieke sector als bij de markt. Dus we zullen ook moeten zorgen dat het SOC en breed Rijkswaterstaat een aantrekkelijke werkgever blijven. Aan iedereen met interesse in dit onderwerp die hier nu mogelijk naar kijkt, zou ik een oproep willen doen. Dit is echt in het belang van Nederland, dus als je nou ergens je kennis en je capaciteiten voor de hele samenleving goed van nut wil laten zijn, is dit een prachtige omgeving om te komen werken.

Mevrouw **Van Brenk** (50PLUS):
Ter afsluiting. Ik begrijp dat de minister goed werkgeverschap wil belonen, dus ik neem aan dat het salaris dan ook navenant is en dat er een prachtige nieuwe cao komt.

Minister **Van Nieuwenhuizen-Wijbenga**:
Daar wordt door andere collega's heel hard aan gewerkt.

De heer **Drost** (ChristenUnie):
Ik was ingegaan op de faalkans van vitale waterwerken. De faalkans is de kans die bestaat dat een vitaal waterwerk faalt op het moment dat wij het nodig hebben. Je kunt je voorstellen dat het risico op cyberaanvallen doortelt in zo'n faalkans. Ik noemde een specifieke kering. Ik kan me voorstellen dat de minister zegt: ik ga niet in op specifieke gevallen. Dat is ook niet mijn vraag. Maar in het algemeen kunnen die faalkans en die kans op cyberaanvallen vervolgens doorwerken in het beveiligings- of het beschermingsniveau van ons land. Dat geeft vervolgens ook de prioriteit aan die we er wellicht aan moeten hangen. Kan de minister daar iets over zeggen? Als het te technisch is, mag het antwoord ook schriftelijk of in tweede termijn, maar die vraag had ik wel neergelegd.

Minister **Van Nieuwenhuizen-Wijbenga**:
Ik hoop dat ik hem zo kan beantwoorden. Ik denk dat de heer Drost een terecht punt markeert. Waar de faalkans vroeger vooral was gericht op de techniek, op de hardware, kan dat echt niet meer in de huidige tijd, want je bent zeker zo kwetsbaar, misschien zelfs kwetsbaarder, op de softwarekant, juist vanwege die cybersecurity. Dat wordt dus nadrukkelijk ook meegenomen in de nieuwe faalkansberekening, want dat moet, omdat die kwetsbaarheid er wel degelijk in zit. Dus de faalkans gaat niet alleen uit van de hardware. De software wordt daar echt in meegenomen.

De **voorzitter**:
Als er verder geen vragen zijn van de kant van de Kamer, dan kunnen we overgaan naar de tweede termijn van de kant van de Kamer. De spreektijd is anderhalve minuut. Daarbinnen moeten ook eventuele moties worden ingediend. Ik zal alleen maar vragen toestaan die verhelderend zijn voor het begrip van de eventueel in te dienen moties. Het woord is aan de heer Von Martels van het CDA.

De heer **Von Martels** (CDA):
Dank u wel, voorzitter. Ik zeg de minister hartelijk dank voor de duidelijke beantwoording. Dat neemt niet weg dat ik toch nog twee moties zou willen indienen. De eerste luidt als volgt.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat bij een cyberaanval op vitale waterwerken andere vitale sectoren, zoals woongebieden, bedrijfsterreinen, verbindingen en luchtvaart, ook geraakt kunnen worden (de zogenaamde cascade-effecten);

verzoekt de regering om de effecten op andere vitale sectoren van een cyberaanval op waterwerken in 2019 in beeld te brengen en daarbij voorstellen te doen om geëigende maatregelen te nemen om die gevolgen te voorkomen dan wel te mitigeren,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Von Martels en Geurts. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 75 (30821).

De heer **Von Martels** (CDA):
De volgende motie, voorzitter.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de Algemene Rekenkamer in het rapport "Dijkverzwaring: cybersecurity en vitale waterwerken" een achttal concrete aanbevelingen doet die door de minister zijn onderschreven;

verzoekt de regering de uitvoering van de onderschreven aanbevelingen voor de zomer van 2020 te evalueren en de resultaten aan de Kamer te melden,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Von Martels en Geurts. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 76 (30821).

Dan kunnen we door naar de inbreng in tweede termijn van mevrouw Van Brenk van 50PLUS.

Mevrouw **Van Brenk** (50PLUS):
Voorzitter. Ik ben blij met de toelichting van de minister dat het niet haar bedoeling is om te wachten, dat we een jaarlijkse rapportage krijgen en dat het budget toereikend is. Omdat het budget toereikend is en de minister ambities heeft, de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat de Algemene Rekenkamer heeft geconstateerd dat met het programma Beveiligd Werken Rijkswaterstaat (BWR) een inhaalslag is gemaakt op het gebied van de cybersecurity van vitale waterwerken;

overwegende dat de ambitie om cyberaanvallen direct te kunnen detecteren, eind 2018 nog niet was gehaald, terwijl dit volgens planning al eind 2017 voltooid had moeten zijn;

overwegende dat hierdoor het risico ontstaat dat een cyberaanval op een vitaal waterwerk niet of niet bijtijds wordt geconstateerd;

verzoekt de regering concreet aan te geven welke acties zij onderneemt om de doelen die eind 2017 al behaald hadden moeten zijn, voor eind 2019 alsnog te behalen, indien dit nodig blijkt de benodigde middelen hiervoor vrij te maken, en de Kamer zo spoedig mogelijk te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Van Brenk. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 78 (30821).

Mevrouw **Van Brenk** (50PLUS):
Voorzitter, nog één motie omdat ik toch meer zekerheid wil, maar misschien kan de minister het toelichten. Dan ben ik graag bereid om haar weer in te trekken.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de minister de opvolging van de aanbevelingen van de Algemene Rekenkamer uit het rapport Digitale dijkverzwaring min of meer afhankelijk maakt van een nieuw op te stellen dreigingsbeeld;

spreekt uit dat maatregelen voor een optimale cybersecurity niet geformuleerd en uitgevoerd kunnen en mogen worden op basis van een dreigingsbeeld, maar op basis van de optimale veiligheidssituatie,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Van Brenk. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 77 (30821).

Dan kunnen we door naar de inbreng van de heer Dijkstra in de tweede termijn. De heer Dijkstra is van de VVD.

De heer **Remco Dijkstra** (VVD):
Ja, nog steeds, voorzitter; daar voel ik me wel thuis. Ik dank de minister voor de beantwoording. Ik dank ook mijn collega's. We hebben met de acht serieuze partijen in de commissie I&W toch een mooi debat op de inhoud gehad. Dat geldt ook voor wat eraan voorafging. Het is wel fijn dat we de politiek en de inhoud mooi met elkaar kunnen combineren. Ik heb het gevoel dat we de urgentie met elkaar delen. Er is ook veel eensgezindheid. Dat is ook niet vreemd als je je bedenkt wat een vreemde mogendheid zou kunnen doen, of dat iemand iets in de software of wat dan ook installeert wat later geactiveerd wordt of dat die ergens binnendringt. Dat heeft dan grote gevolgen. Dan zitten we in een soort James Bond-scenario, een eng boek of een enge film, en we hebben niet een soort James Bond die dan de boel komt redden in anderhalf uur. Nee, dan staat het land half onder water. Dat moeten we niet hebben. De minister moet ons land dus beschermen, met alle mensen die daarvoor dagelijks aan de lat staan. Ze moet ons land veilig houden, de mensen, de bedrijven en de bezittingen.

Het is ook goed om te horen — dat was nieuw voor me — dat die 95 miljoen inderdaad terechtkomt bij die 4, 6 en 7 miljoen extra voor de beveiliging. Ik heb uit de beantwoording ook een beetje begrepen dat de minister de toezegging heeft gedaan om jaarlijks te rapporteren over de hardware, de software en de mindware van mensen en ook over de budgetten. Als u nog andere zaken tegenkomt, naast de aanbevelingen die we al hebben, gaat u die ook melden, heb ik begrepen. Dat is mooi. Daar hoef ik dus geen motie over in te dienen.

De **voorzitter**:
Dank u wel, meneer Dijkstra. Dan is het woord aan de heer Stoffer van de SGP.

De heer **Stoffer** (SGP):
Voorzitter. Volgens mij heeft deze minister van mij geen moties nodig om aangespoord te worden om hier hard aan te werken. In de beantwoording heb ik gemerkt dat dat eigen passie en eigen drive is. Toch een korte afronding van dit debat. Op waterwerken zijn we als Nederlanders trots. We vinden ze mooi. Maar over het algemeen hebben we het er niet vaak over, tot het moment dat ze wat anders doen dan je zou willen dat ze doen. Volgens mij was dit ook onderwerp van het debat, en moeten we met elkaar alle hens aan dek hebben om dat te voorkomen. Dat hebben we vanmiddag ook laten zien.

Ik heb nog één ander punt; ik kan het niet laten, voorzitter. Als die waterwerken niet doen wat je wilt, omdat ze niet goed onderhouden zijn, is dat natuurlijk een nadrukkelijk punt. Volgens mij is dit debat dus ook een mooie opmaat naar volgende week. Dan kunnen we met elkaar gaan werken aan voldoende geld om ze ook gewoon te laten doen wat we willen dat ze doen. Maar daar gaan we eerst een Hemelvaartsweekend over nadenken, dus tot zover dank. Bij dezen mijn tweede termijn.

De **voorzitter**:
Dank, meneer Stoffer. De heer Schonis, D66.

De heer **Schonis** (D66):
Dank u, voorzitter. Dank aan de minister voor de beantwoording van de vragen. Ik ben blij met de toezegging van de minister dat ze straks jaarlijks zal rapporteren over de voortgang van het uitvoeren van de cybersecuritymaatregelen en dat daar dan ook structureel geld of in ieder geval investeringsruimte voor gevraagd wordt. Het doen van pentesten is uiteindelijk toch een essentieel onderdeel van een samenhangende aanpak op het gebied van cybersecurity. Daarom heb ik ook een motie voorbereid. Net als mevrouw Van Brenk hoop ik dat de minister die ter plaatse omarmt, maar we gaan het zien.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat uit het onderzoek van de Rekenkamer over cybersecurity van vitale waterwerken blijkt dat het doen van zogenaamde penetratietesten (pentesten) bij enkele waterwerken risicovol kan zijn;

overwegende dat het doen van pentesten bij alle waterwerken integraal deel uit moet maken van een allesomvattend systeem van cybersecurity;

verzoekt de regering het doen van een volwaardige pentest op de industriële automatiseringssystemen van de vitale waterwerken een integraal onderdeel te laten uitmaken van de cybersecuritymaatregelen bij alle vitale waterwerken,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Schonis. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 79 (30821).

De heer **Schonis** (D66):
Dank u wel.

De **voorzitter**:
Dank u wel, meneer Schonis. Dan krijgen we mevrouw Kröger van GroenLinks.

Mevrouw **Kröger** (GroenLinks):
Voorzitter. Geen moties van mijn kant, maar wel nog twee vragen. De eerste was eigenlijk over hoe de minister wil omgaan met al die verouderde automatiseringssystemen en hoe dat zich relateert aan de cybersecurity.

Dan nog een vraag. De minister ziet hier een heel erg eensgezinde Kamer. We hebben volgens mij niet zo vaak debatten waar we zo eensgezind een probleem onderschrijven, zoals nu bij dit serieuze rapport van de Rekenkamer over de zorgelijke situatie. Mijn vraag aan de minister is of zij ons in de tweede termijn wat kan meenemen naar aan-

leiding van het rapport en de aanbevelingen van de Rekenkamer. Stel de minister heeft drie jaar lang de rapportages gedaan en er was ook nog een beetje geld beschikbaar, waar staan we dan over drie jaar? Wat hebben we gerealiseerd en wat zou het rapport van de Rekenkamer over drie jaar concluderen? Heel graag dit vergezicht van de minister in de tweede termijn.

Dank u wel, voorzitter.

De **voorzitter**:
Dank, mevrouw Kröger. Dan de heer Drost van de ChristenUnie.

☐

De heer **Drost** (ChristenUnie):
Dank u wel, voorzitter. Ik dank de minister voor de beantwoording van de vragen. Ik kom even terug op het puntje faalkans tegen cybersecurity. De cybersecurity die wij met elkaar in dit land voorstaan, moet dermate goed zijn dat de faalkans van onze vitale waterwerken niet afneemt — eigenlijk moet ik zeggen niet toeneemt — en daarmee het beschermingsniveau van ons land niet afneemt. Dat is waarschijnlijk op dit moment nog niet helemaal het geval, want anders stonden wij hier vandaag niet over dit onderwerp te debatteren. Als dat wel zo is, dan hoor ik dat natuurlijk graag van de minister in tweede termijn. Ik heb daar geen motie over, omdat wij er alle vertrouwen in hebben dat de minister met de aanbevelingen die zij op dit moment overneemt en ook de dingen die zij al deed, het goed doet; zij pakt het voortvarend op. Daarmee zien wij uit naar de eerstvolgende rapportage op dat vlak.

Dank u wel, voorzitter.

De **voorzitter**:
Dank, meneer Drost. Daarmee zijn we aan het eind gekomen van de tweede termijn van de kant van de Kamer. Ik kijk even naar de minister of zij in de gelegenheid is om onmiddellijk te reageren. Dat is niet het geval, dus wachten wij eventjes.

De vergadering wordt van 16.43 uur tot 16.55 uur geschorst.

De **voorzitter**:
We gaan luisteren naar de beantwoording en de beoordeling van de moties. Ik geef het woord aan de minister.

☐

Minister **Van Nieuwenhuizen-Wijbenga**:
Dank u wel, voorzitter. Ik dank de Kamerleden voor de zeer positieve inbreng in het debat. Die geeft het gevoel dat we hier eensgezind in optrekken.

Voordat ik op de moties inga, kom ik nog even op de twee vragen die mevrouw Kröger heeft gesteld. Allereerst kwam ze terug op de legacy en de oude systemen die er nog zijn. Zij vroeg hoe ik omga met de vervanging daarvan. Als we maar enigszins het gevoel hebben dat ze kwetsbaar zijn, gaan we ze vervangen. Als dat niet nodig is omdat het standalone is en er een back-up is, doen we dat nog niet. Daar wordt van geval tot geval naar gekeken. Er wordt verstandig mee omgegaan. Kennelijk heeft mevrouw Kröger hierover een vraag.

Mevrouw **Kröger** (GroenLinks):
Als je als bedrijf of wat dan ook een automatiseringssysteem uit de jaren tachtig hebt, is dat toch sowieso iets kwetsbaars? Dat moet je dan toch op termijn vervangen? Dat zijn toch kosten waar we gewoon plannen voor moeten hebben, nog even los van de cybersecurity?

Minister **Van Nieuwenhuizen-Wijbenga**:
Natuurlijk, dat is ook zo. Daar wordt naar gekeken. Er wordt goed in de gaten gehouden of het systeem voldoende functioneert. Je hebt natuurlijk altijd een back-up nodig. Als je een goede back-up hebt, hoef je het niet altijd à la minute te vervangen, afhankelijk van het soort systeem. Dat wordt van geval tot geval serieus beoordeeld. Natuurlijk gaat ook dit mee in het hele verhaal over beheer en onderhoud. De heer Stoffer preludeerde er al op: daar gaan we volgende week over spreken. Bij beheer en onderhoud gaat het natuurlijk niet alleen over de hardware, maar wel degelijk ook over de software, besturingssystemen, enzovoort. De heer Stoffer heeft helemaal gelijk dat je ook zonder cyberdreigingen moet borgen dat het systeem altijd doet wat het moet doen.

Mevrouw **Kröger** (GroenLinks):
Zeker. Het wordt dus niet à la minute vervangen, maar de minister erkent wel dat deze zeer sterk verouderde systemen vervangen moeten worden. En er is ook een plan over hoe, wat en wanneer dat gaat gebeuren.

Minister **Van Nieuwenhuizen-Wijbenga**:
Dat is onderdeel van het geheel van beheer en onderhoud. Op een gegeven moment kom je dan vanzelf bij het blokje vervanging en renovatie terecht. Geen enkel systeem houdt het natuurlijk voor de eeuwigheid vol, en zeker software niet.

Mevrouw Kröger heeft nog een vraag gesteld. Ik moet zeggen dat dat een heel moeilijke vraag is. Wat zie ik over drie jaar voor mij? Het is altijd heel ingewikkeld om in te schatten hoe de wereld er dan uitziet. Ik vind het in ieder geval belangrijk om binnen drie jaar hopelijk vast te kunnen stellen dat de acties die we met de waterschappen in het Bestuursakkoord Water hebben afgesproken ook zijn uitgevoerd. Dan hebben we meer zicht op de hele waterketen. Dat hoop ik over drie jaar in ieder geval bereikt te hebben.

Natuurlijk hoop ik dat we over drie jaar de aanbevelingen van de Rekenkamer hebben opgevolgd. Ik hoop ook dat we tegen die tijd "security by design" overal in onze organisatie hebben ingebed en dat dit bij alles wat we doen vanaf het begin onderdeel van de afweging is. Ik hoop dat we dan niet alleen bij RWS, maar ook op het ministerie een goed niveau van awareness hebben en dat iedereen hier alert op is.

U gaf zelf aan dat de dreiging voortdurend van aard en omvang kan veranderen. Daarom hoop ik dat we ons systeem dan adaptief hebben gemaakt, zodat we steeds op die veranderende omstandigheden kunnen inspelen. Mijn ultieme beeld is natuurlijk dat, als het nou ergens in de

wereld goed voor elkaar is met de cybersecurity van de vitale werken, dit in Nederland is. Daarom wil ik natuurlijk graag blijven leren, niet alleen van wat andere departementen of andere Nederlandse instanties doen, maar ook van bijvoorbeeld een organisatie als ENISA, dat dit Europabreed in kaart brengt. De wereld verandert in termen van cybersecurity namelijk zo snel dat je dit als land niet in je eentje kunt bijhouden. Je hebt internationale samenwerking nodig om zo alert mogelijk te blijven. Want, helaas, de bad guys hebben de neiging om altijd net een stapje harder te rennen, dus daar moeten we met z'n allen bovenop blijven zitten. Dat is het beeld dat ik hoop te hebben bereikt over drie jaar.

Mevrouw **Kröger** (GroenLinks):
Ja, dat is een aantrekkelijk beeld, een belangrijk beeld en een beeld waarvan ik denk dat ook de Kamer wil dat dat bereikt wordt. Misschien is mijn vraag, die er natuurlijk onder zit, dan eigenlijk: als je schetst waar je over drie jaar zou moeten zijn, hoe vertaal je dat dan in concrete doelen en indicatoren waardoor je daar ook doelmatig, doeltreffend en efficiënt kan komen? Dus hoe worden de aanbevelingen van het rapport vertaald naar waar je over drie jaar wil zijn? Wanneer kunnen we die slag als Kamer verwachten?

Minister **Van Nieuwenhuizen-Wijbenga**:
We moeten heel hard aan de bak om alle aanbevelingen van de Rekenkamer op te volgen. Daar kom ik zo meteen bij de moties ook op terug; daar gaan we met volle kracht op inzetten. Maar ik stel me voor dat we ook terugkomen op de hogere ambities die we daarna hebben, ook in die rapportages die ik net heb toegezegd. Het moet niet alleen een afvinklijstje worden, zo van: goh, hoe staat het met aanbeveling X of Y? We moeten ook onze eigen doelstellingen opschrijven.

De **voorzitter**:
Mevrouw Kröger, tot slot.

Mevrouw **Kröger** (GroenLinks):
Tot slot. Daarbij moeten die eigen doelstellingen zo concreet mogelijk worden geformuleerd als echt bereikbare doelen. Want volgens mij is in andere rapportages van de Rekenkamer toch de kritiek op het beleid dat we het onvoldoende borgen in concrete, meetbare doelen, voor over bijvoorbeeld drie jaar.

Minister **Van Nieuwenhuizen-Wijbenga**:
Ik begrijp het punt van mevrouw Kröger heel erg goed. Ook daar speelt natuurlijk toch wel de ingewikkeldheid. Veiligheid kun je ook niet makkelijk in procenten weergeven. Kijk, iets waar u ons op af kunt rekenen is of alle werken dan op het SOC zijn aangesloten. Er zijn gewoon keiharde prestaties die je daarin op kunt nemen. We zullen kijken wat we in dat soort kengetallen kunnen vatten, en wat we misschien wat meer kwalitatief moeten omschrijven. Maar ik begrijp de wens en we gaan kijken wat we daaraan kunnen doen. Want het is voor onszelf ook belangrijk om te kunnen zien of we voldoende grip op alles hebben.

Voorzitter. Ik kom op de moties. De eerste is van de hand van de heer Von Martels. Die verzoekt de regering om de effecten op andere vitale sectoren van een cyberaanval op waterwerken in 2019 beeld te brengen en daarbij voorstellen te doen om de geëigende maatregelen te nemen om die gevolgen te voorkomen dan wel te mitigeren. In de eerste termijn heb ik u aangegeven dat het geheel van de cascade-effecten onder de portefeuille valt van collega Grapperhaus. Maar als u bedoelt dat wij vanuit de waterwerken aan het ministerie van JenV zullen aangeven wat er dan zou gebeuren, dan ben ik natuurlijk graag bereid om dat te doen. Maar als het gaat om wat dat precies voor effecten heeft in die andere sectoren, bijvoorbeeld de telecom, dan zijn natuurlijk de collega's bij EZK veel meer aangewezen om die effecten in beeld te brengen. Dat geldt ook als het gaat om economische effecten. Dus in ieder geval is er zeker de bereidheid om aan te geven welke consequenties er kunnen zijn. Wat dan precies de effecten zijn op die sectoren, moeten die sectoren zelf natuurlijk in kaart brengen.

De **voorzitter**:
Meneer Von Martels, kunt u zich vinden in de uitleg die de minister geeft aan uw motie?

De heer **Von Martels** (CDA):
Ja, inderdaad. Ik hoop natuurlijk dat de minister het zo breed mogelijk oppakt, maar ik ben het eens met de woorden dat ze in ieder geval voor haar eigen ministerie duidelijk zal maken wat de consequenties zijn. Dus in dat opzicht is de motie ook zo bedoeld.

Minister **Van Nieuwenhuizen-Wijbenga**:
Als ik de motie zo mag interpreteren, dan kan ik het oordeel aan de Kamer laten. Want ik kan natuurlijk niet verder gaan dan wat wij vanuit ons ministerie, vanuit Rijkswaterstaat, in kaart kunnen brengen. Maar die informatie zal ik graag aanleveren aan collega Grapperhaus.

Ik kom bij motie op stuk nr. 76. Die is ook van de heer Von Martels en verzoekt de regering om de uitvoering van de onderschreven aanbevelingen voor de zomer van 2020 te evalueren en de resultaten aan de Kamer te melden. Het oordeel over die motie kan ik aan de Kamer laten, want het lijkt me een heel reële wens van de Kamer dat ik dat zal doen.

Ik kom op de motie van mevrouw Van Brenk op stuk nr. 78. Die ziet erop dat we moeten realiseren wat voor eind 2017 was gepland. Ik kan helaas niet zeggen dat we alles voor het eind van dit jaar uitgevoerd krijgen. Wat betreft de aansluiting van vitale objecten op het SOC kan ik u geruststellen: ik zeg u toe dat we dat klaar hebben voor de start van het nieuwe stormseizoen. We hebben dat dus voor 1 oktober voor elkaar. Veel van de overige maatregelen zullen we nog wel dit jaar klaar kunnen krijgen. Ik kan de toezegging doen dat ik u een planning doe toekomen over hoe we dan met de andere maatregelen kunnen omgaan.

Mevrouw **Van Brenk** (50PLUS):
Wat mij betreft kan de minister het zo interpreteren als zij aangeeft. Ik vind het belangrijkste dat de aansluiting op het SOC gegarandeerd is. Dat is dus tijdig. Dat vind ik al een grote plus. Als we dan die planning krijgen, vind ik dat ze tegemoetkomt aan mijn motie.

Minister **Van Nieuwenhuizen-Wijbenga**:
Nou, als u dan het stukje over 2019 eruit haalt, dan zeg ik toe dat we proberen om het allemaal zo snel mogelijk duidelijk te maken.

Dan kom ik bij de motie op stuk nr. 77, ook van mevrouw Van Brenk. Daarin staat dat de Kamer uitspreekt dat maatregelen voor een optimale cybersecurity niet geformuleerd en uitgevoerd kunnen en mogen worden op basis van een dreigingsbeeld maar op basis van een optimale veiligheidssituatie. Mevrouw Van Brenk voelde het al aankomen, want ze zei al: ik hoop dat de minister de motie zal omarmen. Dat kan ik ook doen. Ik kan deze motie overnemen. Ik wilde u inderdaad geruststellen: we gaan niet op onze handen zitten totdat we een dreigingsbeeld hebben; we gaan gewoon voluit aan de slag. Ik weet niet of mevrouw Van Brenk bereid is om haar over te nemen?

Mevrouw **Van Brenk** (50PLUS):
Ja, prima.

De **voorzitter**:
Mevrouw Van Brenk, wilt u hierop ... O, ja, u neemt dat zo over. En het oordeel luidt dan, minister?

Minister **Van Nieuwenhuizen-Wijbenga**:
Nou, als de motie overgenomen is, is zij bij dezen afgedaan.

De **voorzitter**:
O ja, oké, sorry. Dan moet ik even kijken of er bezwaar tegen is dat dit op deze manier wordt afgehandeld. Meneer Dijkstra.

De heer **Remco Dijkstra** (VVD):
Nee, bezwaar tegen het overnemen van deze motie heb ik niet, maar mijn opmerking gaat over de vorige motie. Ik heb de minister horen zeggen: als u die datum eruit haalt, wordt het oordeel Kamer. Klopt dat?

Minister **Van Nieuwenhuizen-Wijbenga**:
Ja, dan kan de motie oordeel Kamer krijgen. Over dat jaartal 2019 heb ik aangegeven dat ik het echt niet kan waarmaken om dat allemaal voor het eind van dit jaar te doen. Maar we kunnen de Kamer wel duidelijk maken hoe de planning er dan wél uitziet.

De heer **Remco Dijkstra** (VVD):
En mevrouw Van Brenk gaat de motie aanpassen.

Mevrouw **Van Brenk** (50PLUS):
Ja.

De **voorzitter**:
Maar dan luidt het oordeel van de minister eigenlijk ...

Minister **Van Nieuwenhuizen-Wijbenga**:
Dan kan ik de motie oordeel Kamer geven.

De **voorzitter**:
Dus de minister ontraadt de motie, tenzij die gewijzigd wordt.

Minister **Van Nieuwenhuizen-Wijbenga**:
Dat is ook correct, ja.

Dan de motie op stuk nr. 79, van de hand van de heer Schonis. Die motie verzoekt de regering om het doen van volwaardige pentesten op de industriële automatiseringssystemen van de vitale waterwerken een integraal onderdeel te laten uitmaken van de cybersecuritymaatregelen bij alle vitale waterwerken. Daarbij heb ik ook een "ja, maar"-vraag in de richting van de heer Schonis. Is mijn interpretatie juist dat u eigenlijk bedoelt dat het altijd onderdeel moet zijn van de afweging, maar dat u ook niet voorstelt dat bij ieder onderdeel altijd een pentest moet worden gedaan? Want als u zegt dat we het altijd en overal moeten doen, ook bij de minder belangrijke dingen, dan kan het niet. Maar als u zegt dat het op de vitale onderdelen altijd een onderdeel van de afweging moet zijn, dan zou ik de motie oordeel Kamer kunnen geven. Maar ik kijk de heer Schonis nu even aan.

De heer **Schonis** (D66):
Dat is juist. Dat is inderdaad de bedoeling. Het gaat om de vitale waterwerken.

Minister **Van Nieuwenhuizen-Wijbenga**:
Ja, oké, dan hebben we daar dezelfde opvatting over. Dan is het altijd een integraal onderdeel van de afweging of de pentest wordt toegepast. Ja? Oké.

De **voorzitter**:
En dan is het oordeel dus: oordeel Kamer.

Minister **Van Nieuwenhuizen-Wijbenga**:
Met die inkleuring is het oordeel Kamer.

Dan ben ik erdoorheen, voorzitter.

De **voorzitter**:
Ja, dat lijkt mij dan ook. Daarmee zijn we gekomen aan het slot van dit debat.

De beraadslaging wordt gesloten.

De **voorzitter**:
We gaan even schorsen tot 17.15 uur. Dan vinden er stemmingen plaats over de wijziging van de Meststoffenwet.

En de moties die zonet in dit debat zijn ingediend, komen dan volgende week dinsdag in stemming. Ik dank de minister voor de toelichting.

De vergadering wordt van 17.10 uur tot 17.17 uur geschorst.

Voorzitter: Arib