Tweede Kamer, NAFIN

VERSLAG VAN EEN COMMISSIEDEBAT
Concept

De vaste commissie voor Defensie en de vaste commissie voor Digitale Zaken hebben op 9 april 2025 overleg gevoerd met de heer Tuinman, staatssecretaris van Defensie, over:

- **de brief van de minister van Defensie d.d. 3 december 2024 inzake reactie op het rapport "De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN" van de Algemene Rekenkamer (36592, nr. 8);**
- **de brief van de minister van Defensie d.d. 20 december 2024 inzake beantwoording vragen commissie over de reactie op het rapport "De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN" van de Algemene Rekenkamer (Kamerstuk (36592-8) (36592, nr. 9);**
- **de brief van de staatssecretaris van Defensie d.d. 31 maart 2025 inzake evaluatie NAFIN-storing (36592, nr. 14).**

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

De voorzitter van de vaste commissie voor Defensie,
Kahraman

De voorzitter van de vaste commissie voor Digitale Zaken,
Wingelaar

De griffier van de vaste commissie voor Defensie,
De Lange

Voorzitter: Kahraman
Griffier: Manten

Aanwezig zijn vijf leden der Kamer, te weten: Ellian, Heite, Kahraman, Kathmann en Pool,

en de heer Tuinman, staatssecretaris van Defensie.

Aanvang 10.16 uur.

De **voorzitter**:
Ik open de vergadering van de vaste commissie voor Defensie. Vandaag staat het NAFIN op de agenda. Ik heet de bewindspersoon en zijn ondersteuning van harte welkom bij de commissie. Ik heet ook de Kamerleden van harte welkom. Ik ga ze aan u voorstellen: de heer Pool namens de PVV, mevrouw Kathmann namens GroenLinks-Partij van de Arbeid, mevrouw Heite namens Nieuw Sociaal Contract en de heer Ellian namens de VVD. In de eerste termijn van de commissie heeft u drie minuten spreektijd.

Ik sta drie interrupties toe in deze ronde als deze minder dan 45 seconden duren. Ik tel een interruptie voor twee als die boven de 45 seconden duurt. U heeft dus zelf in de hand of u drie interrupties krijgt of minder. In de tweede termijn krijgt u een minuut spreektijd.

Ik wil beginnen met de inbreng van de heer Pool namens de PVV.

De heer **Pool** (PVV):
Hartelijk dank, voorzitter. Het belang van een solide en betrouwbaar communicatienetwerk kan voor een krijgsmacht niet overschat worden. De geschiedenis staat bol van veldslagen, ja, zelfs hele oorlogen die uiteindelijk werden gewonnen of verloren omdat een van de strijdende partijen een doorslaggevend voordeel had op dit gebied.

Voorzitter. De PVV wil dan ook dat we in Nederland de boel op dit gebied op orde hebben. Echter, het recent verschenen rapport van de Algemene Rekenkamer over de kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN, laat zien dat dit nu nog niet het geval is, terwijl dit netwerk cruciaal is voor onze krijgsmacht. Defensie zelf omschrijft het systeem niet voor niets als "ons eerste wapensysteem". Van de satelliet in het missiegebied tot de marechaussee die de grenzen bewaakt en de luchtverkeersleider die het radarverkeer bekijkt: allemaal zijn ze afhankelijk van NAFIN. De PVV wil dit netwerk dan ook op orde hebben.

Voorzitter. Maar de conclusies van het rapport zijn keihard. Defensie heeft geen strategie voor of visie op de rol en toekomst van het NAFIN. De fysieke beveiliging van het NAFIN is onvoldoende. Het ontbreekt aan militaire regie en controle vanuit Defensie op het netwerk. Een dieptepunt in dit verhaal was de storing van 28 augustus 2024. Deze storing leidde tot grote problemen bij onder andere de Kustwacht, de Koninklijke Marechaussee en Eindhoven Airport. In de Kamerbrief van 20 maart reflecteert de staatssecretaris op deze storing en zet hij de lessen die Defensie hiervan heeft geleerd op een rij. Graag vraag ik de staatssecretaris naar de stand van zaken hieromtrent. Is Defensie nu wel voldoende voorbereid op een dergelijke storing? Hoe staat het met het uitvoeren van de overgenomen aanbevelingen uit het rapport van de Algemene Rekenkamer? Is bijvoorbeeld de detectie en respons op ongeoorloofde toegang tot het netwerk nu wel op orde?

Voorzitter, tot slot. De staatssecretaris laat weten dat Defensie onderzoekt of het netwerk aangemerkt moet worden als vitale infrastructuur. Onderzoek hiernaar mag maar liefst tot de zomer duren. Graag vraag ik de staatssecretaris waarom hij zo lang nodig heeft om tot een conclusie te komen. Natuurlijk moet ons krijgsmachtnetwerk als vitale infrastructuur aangemerkt worden. Regel dit, daartoe roepen wij dan ook op, en graag snel een beetje.

Dank u wel, voorzitter.

De **voorzitter**:
Dank voor uw inbreng. U bleef keurig binnen de tijd. Ik zie dat mevrouw Kathmann een interruptie heeft richting de heer Pool.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ik ben ongelofelijk blij dat de grootste regeringspartij van Nederland de urgentie deelt en dus ook weet hoe cruciaal die digitale infrastructuur is voor onze nationale veiligheid. In de commissie Digitale Zaken spreken wij hier heel veel over. We hebben het ook over de investeringsagenda die nodig is maar ontbreekt. Mijn vraag is: als de PVV de urgentie voelt, wat is dan de visie van de PVV op het NAFIN? Welke investeringen is de PVV bereid te doen om het op orde te krijgen?

De heer **Pool** (PVV):
Dank u wel voor deze vraag. Ik begin natuurlijk met de oproep waar ik mee eindigde: we zien het NAFIN echt als vitale infrastructuur. Dat is de oproep die ik net aan de staatssecretaris heb gedaan. Het onderzoek mag tot aan de zomer duren. Wij willen echt een beetje actie erop. Er moet gewoon gas op de plank, want het is belangrijk. Die urgentie deel ik met uw partij. Wat de investeringen die daarvoor nodig zijn betreft, hoor ik graag of de staatssecretaris zegt: er moet echt nog een heel groot bedrag bij. Op zich verwacht ik dat niet, omdat hij daar natuurlijk ook gewoon budget voor heeft, maar ik hoor het graag als het anders is.

De **voorzitter**:
Er zijn geen interrupties meer richting de heer Pool. Ik had moeten zeggen dat ook de volgcommissie Digitale Zaken hierbij aangesloten is. Mevrouw Kathmann is lid van Digitale Zaken. Ook aan haar van harte welkom in onze commissie. Het is namelijk een belangrijk onderwerp. Digitale Zaken is daarbij ook aangesloten. Dan geef ik graag het woord aan mevrouw Kathmann namens GroenLinks-Partij van de Arbeid.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Dank u wel, voorzitter. "Get used to it" waren de beruchte woorden van minister Van Weel toen in augustus 2024 het defensienetwerk NAFIN was uitgevallen. Cyberexperts door heel Nederland hebben terecht veel van die woorden gevonden. Ik ook. Maar uiteindelijk hebben we allemaal vooral de mouwen opgestroopt om een komma en een "maar" te zetten achter "get used to it". Ja, we moeten eraan wennen, maar we moeten er wel voor zorgen dat we klaar zijn voor grote en kleine storingen.

Dat zijn we niet. Al meer dan een halfjaar gaan alle alarmbellen af. Soms zou ik willen dat experts hun goede en gedegen rapporten over het NAFIN, zoals het rapport van de Rekenkamer, met soundbites zouden maken, waarbij er letterlijk keiharde alarmbellen afgaan als je het oppakt of erdoorheen zit te scrollen. Misschien gaan we dan voor een keer echt reageren zoals het moet. Nu zijn er vooral geen daden, maar wel heel veel woorden. GroenLinks-Partij van de Arbeid wil echte actie en doet vandaag vier voorstellen om het NAFIN te versterken.

Ten eerste vraag ik om een serieus plan. Je kunt namelijk wel zeggen dat de aanbevelingen van de Rekenkamer worden overgenomen, maar dan moet er een plan liggen. Daarin moet staan hoe, in welk tijdpad en met welke investeringen we dat gaan doen.

Ten tweede vraag ik om een vervolgonderzoek. Vraag de Rekenkamer om volgend jaar een soortgelijk rapport te schrijven, om te kijken of de verbeteringen werken. Sluit deze aan op de oefeningen eind 2025.

Ten derde vraag ik om een toekomstvisie. Welke rol speelt het NAFIN over vijf en over

tien jaar in de infrastructuur van Nederland? Blijft het een soort duizenddingendoekje of wordt het een solide defensienetwerk? Dat is een hele essentiële keuze. Het kan niet beide.

Ten vierde vraag ik om een bredere analyse van strategische afhankelijkheden. Defensie mag nooit door storing belemmerd worden. Voer een stresstest uit van het NAFIN. Stel jezelf de vraag: wat gebeurt er binnen Defensie als er bijvoorbeeld een storing is bij Microsoft of als iemand ergens een stekkertje uit trekt?

Tot slot. Ik hoef de staatssecretaris niet uit te leggen dat digitale infrastructuur ook een onderdeel is van onze nationale veiligheid. Mijn fractie wil dat Defensie zich structureel bemoeit met digitale infrastructuur. Doe mee aan gesprekken over bijvoorbeeld het leggen van nieuwe zeekabels of het ontwikkelen van de AI-faciliteit.

Ik zeg dit eigenlijk allemaal uit een bepaalde trots. Het NAFIN is een voorbeeld van een sterk netwerk in ons eigen beheer. Er werken allemaal getalenteerde, megaslimme mensen om dit draaiende te houden. Geef die mensen een positie en luister naar hun aanbevelingen en rode vlaggen. Zo wordt het NAFIN weer het boegbeeld dat het hoort te zijn.

Tot slot heb ik nog twee praktische, technische vragen. Gebruikt de staatssecretaris inmiddels een veiligere vorm van tijdsynchronisatie binnen het NAFIN? Heeft u inmiddels redundante back-upvoorzieningen ingericht voor tijdsignalen?

De **voorzitter**:
Dank aan mevrouw Kathmann voor haar inbreng. U bleef keurig binnen de tijd. Mevrouw Kathmann had nog 2 seconden over, dus ze heeft het perfect getimed. Ik ga door naar mevrouw Heite namens Nieuw Sociaal Contract.

Mevrouw **Heite** (NSC):
Dank u wel, voorzitter. Het is al vaker gezegd: we leven niet in oorlog, maar ook niet in vrede. We bevinden ons in een zeer gespannen geopolitieke situatie. Het incident afgelopen augustus met het NAFIN-netwerk en de conclusies uit het rapport van de Algemene Rekenkamer laten ons zien dat we militair gezien onvoldoende alert zijn op risico's van sabotage door statelijke actoren. We hebben nog heel wat werk te verzetten om onze samenleving te beschermen tegen cyberaanvallen. Dat baart NSC grote zorgen.

Hoewel het bij dit incident niet om een cyberaanval ging, werd de samenleving wel geconfronteerd met de kwetsbaarheid van het huidige netwerk. We kregen een voorzichtig inkijkje in wat de gevolgen van zo'n aanval zouden kunnen zijn. Het is goed om te lezen dat Defensie onderzoekt of NAFIN niet aangemerkt moet worden als vitale infrastructuur. Wanneer kunnen we de conclusies uit dit rapport verwachten? Waarom wordt NAFIN niet nu al aangemerkt als vitale infrastructuur? In ieder geval ben ik blij met de inzet van de staatssecretaris en de minister om in deze uitdagende tijden alle zeilen bij te zetten om Defensie te versterken.

Voorzitter. NSC heeft in een vorig debat de minister verzocht om het Defensie Cyber Commando te versterken en een adequaat mandaat te geven, zodat het, indien nodig, snel kan schakelen. Daarbij hebben we gevraagd om het aantal cyberreservisten op te

schalen en bij dit alles te zorgen voor passend toezicht. Dit heeft natuurlijk ook alles te maken met de beveiliging van NAFIN. Kan de staatssecretaris aangeven of hij al stappen heeft ondernomen voor het uitwerken van een strategische visie op het functioneren van het NAFIN-netwerk in de samenleving, zoals genoemd in het rapport van de Algemene Rekenkamer? Kan hij aangeven hoe hij uitvoering gaat geven aan de genoemde motie over het versterken van het cyberdomein, de digitale weerbaarheid van Nederland en de opschaling van het aantal cyberreservisten? Kan de staatssecretaris toezeggen dat de Algemene Rekenkamer over twee jaar weer onderzoek doet, om ervoor te zorgen dat de benoemde, terechte veiligheidsrisico's nu wel zijn opgelost?

In het rapport van de Algemene Rekenkamer wordt ook geconcludeerd dat er bij het afhandelen van de storing te laat is gereageerd en dat er onvoldoende aandacht is geweest voor mogelijke cyberrisico's. Gaat de staatssecretaris onderzoeken wat er nodig is bij Defensie met betrekking tot cyberexpertise en het Joint Informatievoorziening Commando om bij een volgende storing adequaat te kunnen reageren en te voorkomen dat weer een deel van de samenleving ernstig wordt ontwricht? Is er voldoende zicht op welke vitale infrastructuren gebruikmaken van NAFIN, zoals andere gekoppelde civiele locaties? En houdt de staatssecretaris daarbij al rekening met de grootschalige uitbreiding van Defensie in de nabije toekomst?

In de initiatiefnota van collega Six Dijkstra wordt een pleidooi gehouden om in het kader van de nationale en internationale weerbaarheid de hoofdverantwoordelijkheid voor de ontwikkeling van toekomstbestendige staatsgeheime informatiesystemen naar het Defensiedomein te brengen, waarbij het ministerie van Defensie een grotere taak krijgt ten aanzien van niet alleen het beschermen maar ook het bevorderen van Nederlandse high-assurance producten. Ook wordt er een pleidooi gehouden om hiervoor middelen in de Defensiebegroting te alloceren. Heeft de staatssecretaris al actie ondernomen richting KPN? Heeft KPN op verzoek van de staatssecretaris al beveiligingsmaatregelen en ABDO-autorisaties doorgevoerd? En vindt hij dit voldoende om het cyberdomein en daarmee de digitale weerbaarheid van Nederland te versterken? Wordt het niet tijd om deze expertise in zijn geheel bij Defensie onder te brengen? En is hij bereid om te onderzoeken wat de mogelijkheden zijn om opvolging te geven aan de oproep in de initiatiefnota van NSC-collega Six Dijkstra?

Tot zover. Dank u wel.

De **voorzitter**:
Dank aan mevrouw Heite. Ik heb u een paar seconden extra gegeven, zeg ik meteen. De volgende keer zal ik dus wat strakker zijn richting mevrouw Heite in verband met de tijd. Dan ga ik over naar de heer Ellian namens de VVD.

De heer **Ellian** (VVD):
Dank u wel, voorzitter. Ik ga proberen binnen de tijd te blijven. Het rapport van de Algemene Rekenkamer over NAFIN legt belangrijke kwetsbaarheden bloot in onze digitale infrastructuur. Defensie zorgt ervoor dat het netwerk regelmatig updates krijgt en aan de laatste technische standaarden voldoet. Maar we zijn bezorgd over de fysieke beveiliging van het netwerk. Uit praktijktesten bleek namelijk dat onbevoegden relatief eenvoudig toegang konden krijgen tot netwerkruimtes van NAFIN. Deze bevindingen sluiten aan bij eerdere constateringen over de beveiliging van militaire objecten in 2022 en 2023. Wat gaat er nu concreet ondernomen worden, en binnen welke termijn, om de

fysieke beveiliging te verbeteren? Het is niet te accepteren dat de bescherming van zulke kritieke infrastructuur vertraagd wordt door administratieve processen, terwijl we weten dat Rusland, China en Iran actief werken aan het ondermijnen van onze nationale veiligheid. We willen snelle en concrete maatregelen en niet nog meer plannen en onderzoeken.

Het rapport toont ook aan dat er geen strategie is voor de rol en toekomst van NAFIN, terwijl dit netwerk van vitaal belang is geworden voor niet alleen Defensie, maar ook civiele overheidsdiensten. De storing van afgelopen zomer heeft de grote impact van een uitval aangetoond. Wij zien de noodzaak, in het verlengde van diverse collega's, om NAFIN direct als vitale infrastructuur aan te wijzen in plaats van eerst onderzoek hiernaar te doen.

Ook maakt het rapport duidelijk dat de afhankelijkheid van KPN en andere onderaannemers problematisch is. Een van de drie hoofdonderaannemers werkte met een verlopen autorisatie zonder dat Defensie dit wist. Wat gaat de staatssecretaris doen om het toezicht op deze partijen te versterken? De aangekondigde maatregelen zijn een stap in de goede richting, maar we willen een concreet tijdpad met duidelijke resultaten en geen vrijblijvende gesprekken. Als NAFIN geen toekomst zou hebben, zoals uit het rapport blijkt, wat dan wel? Wat zijn dan de alternatieven? Gaat er dan een heroverweging plaatsvinden of niet?

Voorzitter. Daarnaast baart de beperkte militaire regie over het netwerk ons zorgen. Hoewel Defensie economisch eigenaar is, heeft het onvoldoende controle over wie er toegang heeft tot het netwerk en wie eraan werkt.

Ook het gebrek aan een alternatief voor civiele gebruikers maakt ons kwetsbaar. We willen dat onderzocht wordt hoe we meer redundantie kunnen inbouwen in deze kritieke infrastructuur, zodat essentiële overheidsdiensten kunnen blijven functioneren als NAFIN uitvalt. De kabinetsreactie erkent de aanbevelingen van de Rekenkamer, maar mist concrete termijnen en prioritering. In deze tijden van toenemende dreigingen en hybride dreigingen verwachten we wel iets meer daadkracht. Er moet nu geleverd worden, niet morgen of overmorgen. De staatssecretaris heeft onze steun voor stevige maatregelen, maar die moeten dan wel snel worden uitgevoerd.

Dank.

De **voorzitter**:
Dank aan de heer Ellian. Inderdaad, u heeft zich keurig aan de tijd gehouden. Dan kijk ik naar de staatssecretaris: hoeveel tijd heeft u nodig om tot beantwoording te kunnen komen?

Staatssecretaris **Tuinman**:
Voorzitter, het gaat echt over onze nationale belangen, dus ik zou willen voorstellen dat ik daar twintig minuten de tijd voor krijg.

De **voorzitter**:
Prima. Dan zijn we hier om 10.50 uur terug voor de eerste termijn van de staatssecretaris.

Staatssecretaris **Tuinman**:
Dank u wel.

De vergadering wordt van 10.32 uur tot 10.52 uur geschorst.

De **voorzitter**:
Ik heropen de vergadering. Voordat ik het woord geef aan de staatssecretaris wil ik aangeven dat de leden in de rest van de vergadering vier interrupties mogen plegen. Daarbij geldt ook de 45 secondenregel. Dan wil ik het woord geven aan de staatssecretaris.

Staatssecretaris **Tuinman**:
Dank u wel, voorzitter. Dank voor de eerste termijn. Het is mooi om te zien dat de heer Ellian tegenwoordig onderdeel uitmaakt van de vaste Kamercommissie Defensie. Ik heb hoge verwachtingen. Ik ben ook heel blij dat mevrouw Kathmann van GroenLinks-Partij van de Arbeid vanuit Digitale Zaken daadwerkelijk hier op deze dossiers aanhaakt. Ik hoop haar ook vaker over dit soort zaken te zien.

Ik zal beginnen met mijn inleiding. Ik heb een aantal mapjes. Ik wil het als volgt doen. Ik begin met NAFIN algemeen. U had ook nog wat specifieke vragen over de opvolging van het onderzoek van de Algemene Rekenkamer, ook op het gebied van onze strategische partner KPN. Dan wil ik tijd besteden aan de interne crisisstructuur en hoe we met de communicatie omgaan. Daarna ga ik in op de digitale weerbaarheid en uiteindelijk de vitaliteit misschien wel van het NAFIN-netwerk. Daarna heb ik nog een aantal afsluitende woorden.

Om te beginnen is de gevechtskracht die de krijgsmacht moet leveren niet alleen afhankelijk van wapens en munitie, maar ook van bytes en bits. Zowel in de oorlogsorganisatie als op het militaire slagveld ontwikkelt de invloed van IT en data zich razendsnel. Dat zien we elke dag weer in Oekraïne gebeuren. De oorlog in Oekraïne is hier misschien wel het sprekende voorbeeld van, waarbij innovatie en technologie een steeds belangrijkere rol spelen, bijvoorbeeld door de inzet van drones, maar ook het gebruik van cloudtechnologie. In de steeds meer gedigitaliseerde wereld is die technologie essentieel geworden of misschien zelfs wel existentieel voor het waarborgen van onze nationale veiligheid, waar mevrouw Kathmann ook aan refereerde. Maar ook het uitvoeren van militaire operaties en het effectief communiceren tussen de verschillende overheidsinstanties en internationale partners is hierbij van belang. Maar ook hierdoor ontstaan weer nieuwe kwetsbaarheden, over het algemeen digitale kwetsbaarheden. IT is ook steeds meer verweven met de kernprocessen in de Defensieorganisatie. Ons militaire NAFIN-netwerk is hier een heel goed voorbeeld van. Ik hoorde de leden van de vaste Kamercommissie dat net ook aangeven. Afgelopen augustus hebben we de gevolgen ervaren van het wegvallen van een belangrijk stuk IT, ook al viel het maar een aantal uur weg. De storing in het NAFIN-netwerk leidde tot grote verstoringen bij onder meer de Koninklijke Marechaussee, de Kustwacht, Eindhoven Airport, meldkamercommunicatie en ook helaas bij Defensie en ons eigen lokale Mulan-netwerk.

Aan de andere kant is NAFIN ook een robuust en betrouwbaar netwerk, waarbij storingen eigenlijk een zeldzaamheid zijn. Het netwerk bestaat nu 26 jaar en heeft geen noemenswaardige downtime gehad, waarbij ik besef dat het afgelopen augustus dertien

uur eruit heeft gelegen. Dat zegt eigenlijk ook wel wat. Dit is ook naar voren gekomen uit het onderzoek van de Algemene Rekenkamer en de externe evaluaties. Die zeggen eigenlijk: dit is wel heel goed ontwikkeld en biedt echt wel een hoogwaardige capaciteit die robuust is. Ik wil ook benadrukken dat het robuuste netwerk een militair netwerk is, zoals meneer Ellian en mevrouw Kathmann specifiek aangaven. Ik zal daar straks op terugkomen. Het is een netwerk van Defensie, ook voor specifieke militaire doeleinden. Daarmee is het cruciaal voor het digitale voortzettingsvermogen van de krijgsmacht. Daarom moeten de robuustheid en betrouwbaarheid van het netwerk geborgd blijven en neem ik lessen mee, zoals u ook allen aangaf, uit deze storing. Eigenlijk zie ik het ook wel als een vorm van een stresstest. De aanzet en het startmoment waren alleen niet op die manier bedoeld. Maar ik zie het wel degelijk als een soort van stresstest. Daarom ben ik blij met de evaluaties die gedaan zijn, door Strict en COT, maar ook door de Algemene Rekenkamer. Die aanbevelingen neem ik over.

Om een concreet voorbeeld te noemen: bij een dergelijk incident is het vaak niet direct duidelijk of de verstoring een cyberincident is of een IT-storing. De externe evaluaties bevelen dan ook aan om één blauwdruk te ontwikkelen voor beide gevallen, dus een IT-storing, die technisch van aard is, of een cyberincident, waar misschien een statelijke of niet-statelijke actor achter zit. Die aanbeveling heb ik dan ook warm omarmd en hebben we op dit moment geïmplementeerd. Dit betekent dat we eigenlijk alle storingen in het netwerk beschouwen als een storing, waarbij we ervan uitgaan dat het allebei kan zijn en we alle voorzorgsmaatregelen treffen.

Zoals ik in de brief heb vermeld, gaan we daarnaast ook vaker dit soort situaties oefenen. Daar zijn we mee gestart. Ik weet uit eigen ervaring dat juist oefenen ervoor zorgt dat je er klaar voor bent op het moment dat het het meest nodig is. Op die manier houden we onze systemen wijs en onze mensen up-to-date en veilig.

Vandaag spreek ik graag ook met u over het belangrijke netwerk en de lessen die ik uit die storing meeneem. Daarbij zal ik, zoals ik ook in mijn brief heb aangegeven, niet ingaan op de specifieke aanbevelingen en conclusies uit de twee onderzoeken die we besloten hebben belegd. Waarom doe ik dat niet? Omdat daar potentiële kwetsbaarheden in staan. Die wil ik niet breed neerleggen. We zijn er namelijk met z'n allen bij gebaat dat we de tegenstander niet wijzer maken dan noodzakelijk is, zeker over zo'n cruciaal netwerk als NAFIN.

Als we het over NAFIN hebben, dan hebben we het over het Netherlands Armed Forces Integrated Network, een datatransportnetwerk dat veilige communicatie tussen de Defensieonderdelen mogelijk maakt. Dat staat volledig los van de reguliere publieke glasvezelnetwerken, waar de gemiddelde burger gebruik van maakt. Daarmee is het eigenlijk ook een vorm van soevereiniteit. Dit netwerk is een publiek-private samenwerking tussen Defensie en KPN. Defensie is daarbij de economische eigenaar van het netwerk. We hebben ook de exclusieve, tot in de eeuwigheid durende gebruikersrechten. Andere gebruikers van de overheid die aan NAFIN verbonden zijn, zijn diverse vitale processen zoals meldkamers.

Toch gebeurde op 27 augustus datgene wat niemand wenste te gebeuren. Dat is ook de reden dat we hier vandaag bij elkaar zitten. Dinsdag om 22.00 uur maakte de Kustwacht als eerste een melding van technische problemen. Rond 2.00 uur 's nachts werd duidelijk dat er op grote schaal een probleem was. Tussen 6.00 en 7.00 uur in de

ochtend op de 28ste werd opgeschaald naar een bestuurlijke crisis van Defensie. Tevens hebben we direct specialisten aan het werk gezet om onderzoek te doen naar dit technische probleem.

Tijdens dit onderzoek werd het technische probleem snel gevonden en nog voor de middag waren de eerste delen van het netwerk weer beschikbaar. Die verstoring bleek gestart met een softwarefout in de firewalls, zoals mevrouw Kathmann ook aangaf. Uiteindelijk ging het mis met de tijdklokken. Door de cybersecurityprogramma's die we eroverheen draaien, begon het netwerk zichzelf uit te schakelen op basis van een veiligheidsbepaling. De technische oorzaak was uiteindelijk na dertien uur opgelost. Dit duurde langer dan wij acceptabel vinden; daar ben ik eerlijk over. In de agreements omtrent NAFIN hebben we afgesproken dat we er altijd van uitgaan dat het niet langer mag duren dan vier uur. Er is dus wat te leren.

De belangrijkste lessen uit de evaluatie accepteer ik. Die neem ik ook over. Ik zie de storing van NAFIN als iets wat te betreuren valt, maar ook gewoon, zoals mevrouw Kathmann daarstraks ook aangaf, als een stresstest waardoor we met z'n allen weer op "aan" staan en moeten blijven staan. We moeten zorgen dat we het voor de toekomst beter regelen. Met andere woorden, we moeten beter voorbereid zijn op IT- en cyberincidenten. Zoals ik aangaf, behandelen we die nu op dezelfde manier. We moeten sneller handelen in het geval van IT- en cyberincidenten; daar kom ik zo meteen nog op terug. Deze lessen neem ik dan ook niet lichtzinnig. Ik heb ook maatregelen genomen om dat snel te verbeteren.

Om op die maatregelen terug te komen: ik denk dat de belangrijkste maatregel die we nemen, is dat we beter voorbereid zijn en onze continuïteitsplannen daarin verbeteren. Die vormen ook de blauwdruk bij een uitval van onze systemen. Ik kom daar straks in de specifieke beantwoording van uw vragen nog verder op terug. Bij het herzien van deze plannen ga ik prioritering aanbrengen. Dat heb ik eigenlijk al gedaan, moet ik eerlijk zeggen. Ik ben namelijk ook van "liever daden dan woorden". Daarom doe ik dat nu. We hebben die prioritering aangebracht. Dat betekent dat we voor onszelf helder hebben welke cruciale systemen we als eerste opstarten. Dat betekent wel dat minder urgente systemen — dat kan een Mulan-netwerk zijn, dus mijn eigen gebruikers — pas later weer online komen.

We moeten ook zorgen dat het crisiscommunicatieplan beter wordt opgesteld. Een van de zaken waar het nog misging, is heel praktisch. We zitten in die hele digitaliseringsmove, dus onze sneeuwballijst, die normaal gesproken altijd aan de muur hangt en waar precies op staat wie je moet bellen, zat nu in ons digitale systeem. We waren die dus eigenlijk gewoon een aantal uur kwijt. We zijn daarin niet robuuster gemaakt, maar hebben wel een back-up. We hebben de lijstjes wel degelijk ook weer fysiek opgehangen in de beveiligde ruimtes, zodat we daarmee aan de slag kunnen gaan. Dat doen we ook met interne en externe partners. Ik denk dat de allerbelangrijkste maatregel die ik neem, is dat we dit vaker gaan beoefenen en ook in onze reguliere gereedstelling gaan betrekken. Ook als oud-militair weet ik namelijk als geen ander hoe belangrijk het is om die noodsituaties te oefenen. Door IT- en cyberincidenten vaker te oefenen, zorgen we met z'n allen dat we daar uiteindelijk beter op voorbereid zijn. Volgens mij was dat ook de oproep aan mij, die door allen van u is gedaan.

De **voorzitter**:

Dank voor uw eerste inleidende mapje. De heer Pool heeft daarover een vraag.

De heer **Pool** (PVV):
Dank aan de staatssecretaris voor zijn introductie. Ja, interessant. Maar ik hoor nog niet heel erg concreet of het nou wel of niet is opgelost. De staatssecretaris zegt namelijk dat het dertien uur geduurd heeft, terwijl het maar vier uur mag duren. Is het bij een volgende storing — stel dat het vanavond weer gebeurt — binnen vier uur opgelost of niet?

Staatssecretaris **Tuinman**:
Ik kan dat niet hard beloven, want dan word ik daar de volgende keer door de heer Pool knetterhard op afgerekend. Dat ben ik helemaal met hem eens, maar ik kom zo meteen in de beantwoording van de vragen uiteindelijk wel op wat we gaan doen. Ik wil er wel over zeggen dat een van de redenen waarom het lang heeft geduurd, intern in mijn eigen organisatie ligt en te maken heeft met hoe we hierover communiceren. Onze IT-specialisten, die aan de voorkant van de storing zaten, dachten in eerste instantie dat het een technisch mankement was dat een kleine impact zou hebben. Het heeft dus gewoon te lang geduurd voordat ze dat daadwerkelijk hadden geëscaleerd naar de hogere legerleiding. Dat is dus ook een stukje cultuur. We hebben echt wel hele goede mensen, misschien wel de beste IT'ers, die daadwerkelijk in die systemen zitten. Maar de cultuuromslag is echt wel daar. Het lastige van NAFIN is dat het in de avonduren en in de weekenden gewoon veel minder gebruikt wordt. De traffic is lager en daardoor zie je de impact van dit soort dingen ook minder snel komen. Dat hebben we er ondertussen dus echt wel uitgeramd. Als er iets is, wordt er meteen aan de grootste alarmbellen getrokken. Het crisisteam — het Defensie Beleidsteam, het DBT — wordt uiteindelijk gealarmeerd en daar worden interdepartementaal ook de NCTV en dergelijke direct bij betrokken. Dat zorgt ervoor dat we misschien niet de storing direct kunnen opheffen — dat streef ik natuurlijk wel na — maar voornamelijk dat we de impact van die uitval kunnen minimaliseren.

De **voorzitter**:
Dan heeft mevrouw Kathmann nog een vraag.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik ben eigenlijk wel blij met de inleiding van de staatssecretaris. Als je namelijk echt heel kritisch en een beetje gechargeerd kijkt naar de stukken die we hebben gekregen, dan komen die een beetje over als: nou ja, we hebben een brief naar KPN gestuurd en we gaan wat bewustwordingsdagen doen. Uit de inleiding blijkt wel heel duidelijk dat we veel meer gaan doen. Eigenlijk lijkt het ook een beetje op een soort crisisplan. Dat is heel fijn. Ik weet dat ik normaal gesproken in de commissie Digitale Zaken zit, dus er is een deel dat dan misschien vertrouwelijk moet. Maar is het mogelijk om die crisisplannen dan ook echt als een plan aan de Kamer te presenteren? Ik zou daarin namelijk ook wat duidelijker willen hebben hoe het nou verdergaat met de dienstverlening aan bijvoorbeeld publieke spelers, want daar gebeurt nogal wat. Daar wordt een en ander herzien, of ze worden misschien eerder of later aangesloten bij een storing. Bij het krijgen van meer vertrouwen hoort ook dat we weten dat er echt een plan ligt.

De **voorzitter**:
Ik moet wel aangeven dat mevrouw Kathmann ruim over de 45 seconden is gegaan, dus

deze interruptie reken ik als twee interrupties. Het woord is aan de staatssecretaris.

Staatssecretaris **Tuinman**:
Ik kom zo bij KPN. Die zal ik dan uiteindelijk ook behandelen. U geeft ook aan dat in het parlementaire systeem de Kamercommissie voor Defensie en de Kamercommissie voor Digitale Zaken eigenlijk meer en meer in elkaar overlopen. Daar ging mijn hele inleiding uiteindelijk ook over. Vanavond hebben we natuurlijk nog het debat over hybride dreigingen. Daar zal dat beslist ook ter sprake komen. Niet ik, maar u gaat over uw agenda, maar ik denk wel dat het waardevol is om mij een keer uit te nodigen bij een debat met betrekking tot het thema digitale zaken. Die crisisplannen zijn natuurlijk wel vertrouwelijk, want uiteindelijk willen we die niet aan de grote klok hangen. Maar ik denk dat het misschien wel een weg is als die twee commissies, dus ook die voor Digitale Zaken, daar een keer samen naar kijken als dat opportuun is. Mevrouw Heite vroeg bijvoorbeeld over de KPN of er op verzoek van de staatssecretaris beveiligingsmaatregelen en ABDO-autorisaties zijn doorgevoerd en of we vinden dat het cyberdomein en de digitale weerbaarheid van Nederland daarmee voldoende zijn versterkt. Wij zijn met KPN gestart met het doorvoeren van de maatregelen die uit het onderzoeksrapport van de Algemene Rekenkamer naar voren komen, zoals dat er minder onderaannemers moeten zijn en dat KPN de verantwoordelijkheid heeft, want die is ABDO-gecertificeerd. Daarin zit de regeling dat ze verantwoordelijk zijn voor hoe ze dat met hun onderaannemers doen, en dat zijn niet alleen woorden. Er is een brief over gestuurd en ik heb hierover persoonlijk gesproken met de voorzitter van het bestuur van KPN, de heer Farwerck, en hem dat in niet mis te verstane, klare taal duidelijk gemaakt.

Aan de andere kant is KPN een belangrijke strategische partner. De verstandhouding is eigenlijk wel prima. Ik ben ook wel blij dat we dit met KPN doen, omdat de strategie van KPN is dat het allemaal in Nederland zit, ook als je kijkt naar hoe het eigenaarschap binnen de structuur van KPN is opgebouwd. Het hele netwerk zit in Nederland, dus ik ben wel blij dat we dat samen met hen doen. Elk kwartaal zitten we met KPN om de tafel en dan hebben we het er specifiek over of de stappen zijn gezet die daarvoor noodzakelijk zijn.

Door een aantal woordvoerders is gevraagd of KPN misschien meer activiteiten moet verrichten in dat netwerk. Ik denk eigenlijk dat de relatie die we nu hebben met KPN, prima is. De heer Ellian had daarover ook een vraag. Nogmaals, we hebben diverse maatregelen genomen. KPN is zich terdege bewust van wat dat betekent en wat ze moeten doen. We ontwikkelen samen met KPN een strategische visie op NAFIN, waarover ook een vraag is gesteld, en op het uitbesteden aan minder partijen door KPN en het verbeteren van het toezicht op die externe partijen. Daarover voeren wij ook wel weer audits, om het veiligheidsbewustzijn van medewerkers van KPN en de onderaannemers te verhogen. Dat wat betreft KPN.

De **voorzitter**:
Als u door het mapje KPN bent, dan heeft mevrouw Heite nog een vraag.

Mevrouw **Heite** (NSC):
Mag ik dit ook opvatten als een antwoord op de vraag of de staatssecretaris het niet verstandiger vindt om deze hele expertise onder te brengen bij Defensie? Is het antwoord daarop nee? Is de samenwerking met KPN van strategisch belang en kiest de staatssecretaris ervoor om daarmee door te gaan in plaats van dit in z'n geheel bij

Defensie onder te brengen?

Staatssecretaris **Tuinman**:
De vraag is wat het precies betekent om dat daar volledig onder te brengen. Alles wat wij draaien over dit netwerk is van Defensie. Alle servers en alle aangesloten apparatuur zijn van Defensie. Of iemand er wel of niet op komt, gaat over ons netwerk heen, dus dat wordt samen met de overheid bepaald. Het fysieke netwerk zelf is glasvezel. Er ligt een extensief glasvezelnetwerk door Nederland heen waarop onze defensielocaties aangesloten zijn en waarop een aantal civiele locaties aangesloten zijn, lees: de overheid. Bij die glasvezelkabel zijn dat echt hele fysieke activiteiten. Als wij een nieuwe kazerne of een nieuwe dependance ergens neerzetten, moet die aangesloten worden, en dat doet KPN. Je moet echt met kraantjes in de grond gaan graven. Je moet dat netwerk fysiek aanleggen. Ik zou toch willen voorstellen om dat niet zelf te doen, maar de robuustheid van het netwerk en het netwerk zelf zijn wel degelijk onze verantwoordelijkheid. Ik zou dat ook zo willen doen, want de expertise van het fysieke glasvezelnetwerk hebben wij niet en dat is ook niet nodig. Dat gaat allemaal prima met KPN.

De **voorzitter**:
Ik zie geen vervolgvragen. Dan kunt u door met uw volgende mapje. Volgens mij was dat het Algemene Rekenkameronderzoek.

Staatssecretaris **Tuinman**:
Jazeker, voorzitter. De heer Pool vroeg hoe het staat met de uitvoering van de aanbevelingen van de Algemene Rekenkamer. Die nemen we direct over. We hebben daar direct opvolging aan gegeven in concrete acties en bij de beveiligingsorganisatie. We hebben onze procedures aangescherpt en we sturen op naleving van die procedures. We doen dat ook met die oefeningen en dan komen er toch elke keer weer kleine zaken aan het licht, die we dan ook direct aanpassen. We hebben ook onze veiligheidsprotocollen direct aangepast. Een klein voorbeeld is dat er fysieke papiertjes op de muur zijn, zodat de sneeuwballijst wel te vinden is als het misgaat.

De aanbevelingen over de fysieke beveiliging pakken we ook aan. Daarvoor hebben we een programma ontwikkeld, want dat loopt al langer bij de Algemene Rekenkamer. Het gaat om de onvolkomenheid bij de beveiliging van militaire objecten. De afgelopen tijd hebben we daar echt wel wat stappen gezet, bijvoorbeeld bij de toegangspoortjes, waar de heer Stegeman zich tussendoor kon wringen. Die hebben wij direct allemaal aangepast. Dat doen we zowel fysiek als digitaal. We zijn hiermee gestart en er ook al langer mee bezig wat betreft de cultuur, en daar zijn we nu aan het doorpakken. Het gaat ook om het dragen van je smartcard, en dat we elkaar aanspreken als we iemand zien rondlopen die niet helemaal past in het plaatje of op een bepaalde plaats of tijd. Als iemand die veiligheidsmaatregelen niet neemt, is het cultuur om elkaar daar ook op aan te spreken.

Nogmaals, de aanbevelingen van de Algemene Rekenkamer doen we, wat betreft de fysieke maatregelen. We zijn ook gestart met een onderzoek naar vitaal, waar ik straks nog even op terugkom. Het derde punt was dat we onze onderaannemers ook moesten aanspreken. Dat hebben we gedaan, zowel mondeling als schriftelijk. We hebben daar ook een formele reactie op terug gehad. Uiteindelijk hebben we een proces ingezet dat we er elk kwartaal hard op aansturen.

Mevrouw Kathmann en mevrouw Heite vroegen of we dat soort onderzoek van de Algemene Rekenkamer niet structureel moeten herhalen. Ik wil er wel op wijzen dat het een College van Staat is dat over zijn eigen agenda gaat; dat ten eerste. De Algemene Rekenkamer beslist zelf waar onderzoek naar wordt gedaan. Het aspect fysieke beveiliging en veiligheid is al onderdeel van het jaarlijkse verantwoordingsonderzoek van de Algemene Rekenkamer. We hebben het er al elke twee of drie weken over. Eén ding is zeker in deze tijd: ik ben me zeer bewust van de risico's en de impact van beïnvloeding en sabotage. Dat is toch nog best wel lastig, omdat je moet kijken naar de fysieke en digitale maatregelen die je moet nemen. De allergrootste uitdaging is de culturele omslag.

Ik wil er nog één ding over zeggen, voorzitter. Ik zie ook dat het belangrijk is dat mijn krijgsmacht openstaat voor de samenleving. Dan gaat het ook over de weerbaarheid. Ik zeg wel vaker dat mijn oefenterreinen jullie achtertuinen zijn. Mijn kazernes zijn ook wel een beetje de huiskamers van de samenleving. Maar aan de andere kant moet ik ook gewoon knetterharde beveiligingsmaatregelen doorvoeren en ook een soort Fort Knox om een kazerne heen bouwen. Het is superbelangrijk dat de te beveiligen belangen die we binnen hebben liggen, ook beveiligd blijven en dat die van ons blijven en niet van anderen.

De **voorzitter**:
U bent door uw mapje Algemene Rekenkamer heen?

Staatssecretaris **Tuinman**:
Ja.

De **voorzitter**:
Dan ga ik naar de Kamerleden. De heer Pool had als eerste een vraag.

De heer **Pool** (PVV):
Goed dat de staatssecretaris zegt wat hij allemaal doet, maar ik wil zo graag weten of het voldoende is. Daarom ook hier de concrete vraag of de staatssecretaris kan uitsluiten dat het nu mogelijk is voor iemand om zomaar toegang te krijgen tot het netwerk; ja of nee.

Staatssecretaris **Tuinman**:
De vraag van de heer Pool is of zomaar iemand toegang kan krijgen tot het netwerk. Dat kan ik uitsluiten.

De heer **Pool** (PVV):
Daar is de PVV erg blij mee. Dat is mooi. Alleen, vroeger kon dat dus wel. Dat hebben we geconstateerd bij dit rapport. Mijn vraag is of er in die tijd iets is gebeurd wat kwalijk is. Hebben bijvoorbeeld de Russen of de Chinezen in die tijd gebruikgemaakt van die kwetsbaarheden? Hebben ze bijvoorbeeld een usb-stick ergens achtergelaten in zo'n netwerksysteem?

Staatssecretaris **Tuinman**:
We hebben best wel wat detectiemiddelen en analyses die we over onze systemen heen draaien. Ik ga er niet te veel in detail op in, want dat wil ik eigenlijk niet weggeven. Ik kan

wel zeggen dat we erbovenop zitten, met de detectiemiddelen, de cybersecurity en de digitale tools die we hebben en eroverheen draaien. Als er malign activities zijn, om het in mooi Nederlands te zeggen, dus activiteiten die door kwaadwillenden plaatsvinden, dan pikken we die wel degelijk op. We hebben geen indicaties dat die hier hebben plaatsgevonden. We hebben er best hard op gelopen, om verstoring van NAFIN echt terug te brengen; dat zeggen het onderzoek van de Algemene Rekenkamer en die andere twee onderzoeken eigenlijk ook. Het is een technisch mankement. Het zit in die firewall en in die tijdssynchronisatie. Onze firewalls en onze cybersecuritytools die we draaien, hebben eigenlijk heel goed gefunctioneerd, want die hebben dat gedetecteerd. Er gebeurde iets wat niet oké is en uiteindelijk is het systeem gaan afschalen. Dat heeft heel veel impact, dat hebben we ook gezien. Maar uiteindelijk is het voor mij wel een teken dat als er ergens iets misgaat, het systeem gewoon in een shutdown gaat. Wij moeten ervoor zorgen dat dit niet gebeurt als het niet nodig is. En als het gebeurt, moeten we zorgen dat we heel gauw toolspatches kunnen bouwen. Dat doen we bijvoorbeeld met Cisco, om niet meteen alles open te gooien, maar wel dat veilig op te bouwen en te prioriteren, dus eerst de meest kritieke processen weer online te brengen.

De **voorzitter**:
Dan ga ik naar mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Ik wilde even terugkomen op het Rekenkamerrapport. Als het aan GroenLinks-Partij van de Arbeid ligt, zou dit liefst elk jaar herhaald worden. Ik snap dat we niet een opdracht kunnen geven aan een College van Staat om dat even lekker te doen, maar ik hoop dat de staatssecretaris wel snapt wat de bedoeling daarvan is. Op papier zou dit überhaupt nooit kunnen gebeuren. We hebben op papier allerlei zaken ingebouwd, waardoor dit nooit had kunnen gebeuren. Daarom ben ik het ook helemaal eens met de staatssecretaris dat het gaat om een cultuuromslag. Maar we hebben blijkbaar de hete adem van zulke rapporten nodig om het echt te doorleven, om het echt te gaan doen. Als Kamer kunnen we dan ook controleren of die cultuuromslag er ook echt gaat komen. Is er een mogelijkheid om een onafhankelijke partij over een jaar dezelfde vragen te laten stellen, om te kijken of die cultuuromslag ook echt heeft plaatsgevonden?

De **voorzitter**:
Ik moet helaas weer constateren dat mevrouw Kathmann over de 45 seconden is. Dat betekent dat u door uw interrupties heen bent. De staatssecretaris.

Staatssecretaris **Tuinman**:
Ik denk dat mevrouw Kathmann, net als de hele vaste Kamercommissie die hier aanwezig is, en ikzelf ook, het belang ziet van dit soort systemen. Ze zijn noodzakelijk. We moeten de toepassing maximaliseren, omdat dat in het belang van Nederland is, maar ook zorgen dat ze veilig zijn. Ik onderschrijf volledig wat mevrouw Kathmann zegt. Daarom zei ik ook dat ik die aanbevelingen daadwerkelijk overneem. Die onvolkomenheid is een onvolkomenheid. Voor mij is het een treurpunt en ik werk daar hard aan. Voor u is het misschien precies datgene waar u om vraagt. De Algemene Rekenkamer zal daarover jaarlijks rapporteren, ook met Verantwoordingsdag, dus dat gaat binnenkort komen. Misschien is het mooi om er een balletje over op te gooien in de commissie voor Digitale Zaken, en om die staatssecretaris hiernaartoe te halen, als het gaat om de digitale aspecten van de krijgsmacht.

Ten tweede wil ik zeggen dat ik het heel belangrijk vind en er wel blij mee ben dat wij penetratietesten doen op basis van het rapport van de Algemene Rekenkamer. Deels doen wij dat vanuit onze veiligheidsorganisatie zelf en deels met de Algemene Rekenkamer. Wij doen zelf ook fysieke penetratietesten en daar leren we van. Dat wordt ook gedaan door de mensen van onze eigen beveiligingsorganisatie van Defensie, de DBBO. Daar werken een hoop mensen elke dag knetterhard om onze locaties veilig te houden. Die teams doen hieraan mee en die trainen dus op hun eigen locaties. Het is dus meer dan alleen woorden. We zijn er echt dagdagelijks mee bezig.

De **voorzitter**:
Dan heeft mevrouw Heite nog een vraag richting de staatssecretaris.

Mevrouw **Heite** (NSC):
Eigenlijk heeft mijn buurvrouw dezelfde vraag gesteld als die ik had. Ik heb begrepen dat er in ieder geval aandacht is voor cyclisch hiernaar kijken, dus mijn vraag is beantwoord. Dank u wel.

De **voorzitter**:
Deze reken ik niet als een vraag, omdat het geen vraag is richting de staatssecretaris. Dan ga ik naar de heer Ellian.

De heer **Ellian** (VVD):
Ik heb een vraag, maar ik weet even niet bij welk mapje we zijn.

Staatssecretaris **Tuinman**:
Ik heb er nog twee. Eentje gaat over de crisisstructuur en eentje over het wel of niet vitaal verklaren.

De heer **Ellian** (VVD):
Oké. Ik heb een vraag over KPN en onderaannemers. Past die hier?

De **voorzitter**:
Dat is al geweest, maar ik sta u toe om die vraag te stellen; geen enkel probleem.

De heer **Ellian** (VVD):
Het is nog even wennen, want het is ook meteen diep de techniek in. Al luisterend voel en hoor ik de urgentie, maar het gaat even om de hoofdaannemer en de onderaannemers. De staatssecretaris zegt dat hij in niet mis te verstane bewoordingen de baas van KPN heeft aangesproken. Maar er zit een hele keten aan onderaannemers in, en daar zit een risico. Zou ik Rusland, China of Iran zijn, dan zou ik ergens daarin infiltreren en dan ben je dicht bij het netwerk. Gaat de staatssecretaris hier wat aan doen?

Staatssecretaris **Tuinman**:
Jazeker, meneer Ellian, dat doen we ook. Nogmaals, ik heb Farwerck niet alleen boos aangekeken en wat strenge woorden gesproken. Ik heb hem ook geboden om het aantal onderaannemers terug te dringen. Daarom toetsen we daar elke drie, vier maanden op. Het tweede waar ik hem ook op heb aangesproken, is zijn ABDO-certificering. Die ABDO-certificering is hartstikke prima. De ABDO is overheidsbreed en daar staan regelingen in dat aannemers met onderaannemers daar hun verantwoordelijkheid in

nemen. Dat toetsen we ook. De derde is ook op basis van de wensen van uw Kamer en ook op basis van de serieusheid die dit kabinet betracht, niet alleen met betrekking tot de ABDO. De ABDO gaat namelijk echt over militaire capaciteiten en defensie-industrie; laat ik het zo zeggen. Maar we zijn nu natuurlijk ook bezig met de ABRO, waaraan uiteindelijk ook meer civiele diensten in die keten moeten voldoen. Volgens mij is de brief daarover al richting uw Kamer verstuurd. Ik denk dus wel degelijk dat het niet alleen in woorden zit en dat het meer zoals dat is.

Ik wil ook nog even aangeven dat ook meespeelt dat het in die ABDO ook gaat over het screenen en het certificeren van personeel, ook bij de onderaannemers. Dat toetsen wij ook gewoon. Ze moeten dus uiteindelijk ook gewoon laten zien dat ze de die ABDO-protocollen volgen en daar zitten eigenlijk best wel wat goede zaken in. Ik wil nogmaals echt bevestigen dat KPN een trusted partner is. Ik zie ook wel dat ze dit serieus nemen, ook in hun eigen bedrijfsvoering. Ik ben het er ook over eens dat het niet allemaal makkelijk is. We hebben het met z'n allen over weerbaarheid en hoe we ons beter kunnen beschermen tegen statelijke en niet-statelijke actoren. Ik denk dat we mekaar daarin ook kunnen versterken.

Dan nog een laatste woord daarover. In de samenwerking met KPN, en überhaupt met civiele partijen zoals Microsoft, leren wij heel veel over hoe je dit doet. Die zijn er namelijk dagdagelijks mee bezig. We zien dat KPN soms best slimme dingen heeft, die wij weer over kunnen nemen in onze veiligheidszaken.

De heer **Ellian** (VVD):
Ik ga dit binnen 45 seconden doen.

Helder verhaal. Het is goed dat de staatssecretaris en uiteraard zijn mensen er zo bovenop zitten. In het verlengde hiervan: kwetsbaarheid zit 'm in het infiltreren van zo'n onderaannemer. Maar het is ook zo dat wanneer je afhankelijk bent van zo'n onderaannemer en die onderaannemer uit de keten wordt getikt, je ook weer een probleem hebt. U gaat namelijk niet over die onderaannemer. Is KPN er dus ook van doordrongen dat in de keten die onderaannemers echt moeten leveren, ook als het spannend wordt?

Staatssecretaris **Tuinman**:
Dat vind ik een hele goede vraag, hoor. Dat gaat echt over gegarandeerde capaciteit. Daar zijn ze wel van doordrongen, maar daarom heb je ook van die oefeningen nodig. Dat gaat echt niet alleen om de eigen mensen in onze service, maar dat doe je ook samen met partners. Dat is niet alleen KPN. We hebben bijvoorbeeld Cisco. Die partij is voor ons ook hartstikke belangrijk. Als er ergens iets misgaat, heeft die namelijk een digitaal lab, dat we ook weer kunnen gebruiken om heel snel patches te maken. Het gaat er natuurlijk om dat het hele systeem draait. Ik ben het met de heer Ellian eens dat je nooit van één onderaannemer of één kritieke supplier afhankelijk kunt zijn.

De **voorzitter**:
Ik zie geen vragen meer. Dan kan de staatssecretaris zijn beantwoording voortzetten.

Staatssecretaris **Tuinman**:
Yes, voorzitter. Er waren nog wat vragen over de digitale weerbaarheid en vitaliteit in relatie tot NAFIN. Die vragen waren gesteld door een aantal van u; sowieso door

mevrouw Kathmann en mevrouw Heite, maar eigenlijk ook door meneer Pool. Volgens mij had meneer Ellian het er ook over. Ik heb die vragen een beetje met elkaar samengevoegd tot de vraag: moet NAFIN niet gewoon aangemerkt worden als vitale infrastructuur? We zijn een onderzoek aan het doen. De uitkomst daarvan komt voor het reces en we zullen jullie daar zo spoedig mogelijk ook een brief over sturen, waarin staat wat wijsheid is. Ik wil nog wel zeggen dat het vitaal verklaren van het netwerk ook voor ons niks zegt over hoe vitaal het netwerk is. Wel is het zo dat bij het vitaal verklaren van een netwerk een hele set aan aanvullende en verplichtingen hoort, die komen vanuit de versterkte aanpak beschermde vitale infrastructuur van het ministerie van JenV. We kijken ook of en onder welke voorwaarden we daar op de juiste manier aan kunnen voldoen en op welke termijn dat zou moeten gebeuren. Voor mij staat als een paal boven water dat het een randvoorwaarde moet blijven dat de regie van Defensie op NAFIN daadwerkelijk behouden blijft. NAFIN, Netherlands Armed Forces Integrated Network, is namelijk primair een militair netwerk, zoals een aantal van u ook hebben aangegeven.

Als laatste wil ik daarover nog het volgende zeggen. Defensie is altijd van de contingencies en de dingen die we leren van wat er is misgegaan, zoals het incident van 27 augustus op 28 augustus. Wat ook terugkomt in de onderzoeken is dat je in een crisis een eenhoofdige leiding moet hebben. Het moet dus duidelijk zijn wie erover gaat; die moet daadkrachtig kunnen besluiten en snel kunnen handelen. Vanuit mijn ervaring bij de krijgsmacht, ook als militair, kan ik zeggen dat het goed is als superduidelijk is wie erover gaat. Hoe meer departementen, hoe meer instellingen en hoe meer mensen erbij betrokken zijn aan de voorkant, hoe lastiger het vaak is om uiteindelijk een beslissing te nemen. Het onderzoek vindt nog plaats. Ik wil de Kamer wel meegeven dat ik dit zwaar zal meewegen bij het wel of niet vitaal verklaren van het netwerk, want het zou kunnen betekenen dat je visie, je richting maar voornamelijk ook de regie op het netwerk, zeker in crisissituaties, weleens diffuser zou kunnen worden. Maar goed, dat onderzoek loopt. Dat komt voor het reces, en ik informeer u daar zo spoedig mogelijk over, met de kanttekening dat NAFIN cruciaal, misschien zelfs essentieel, is voor de krijgsmacht, en dat we alle maatregelen treffen die noodzakelijk zijn om dit veilig en functioneel te houden. Het belangrijkste is dat we goed met elkaar in dialoog zijn.

Er was nog een wat breder punt, over de strategische autonomie. Mevrouw Kathmann vroeg: als Microsoft als grote serviceprovider van digitale diensten zou uitvallen, wat doen we dan? Bij Microsoft zit een deel van onze applicaties en werkplekken. Als dat uitvalt, dan is het risico op de korte termijn wel beperkt, want de bedrijfsvoering en de operationele inzet kunnen wel degelijk doorgaan. Daar hebben we namelijk onze eigen IT-infrastructuur voor. Trouwens, daar is het NAFIN dan ook wel weer heel belangrijk voor. Op de wat langere termijn wordt dat risico eigenlijk steeds groter, want de fouten zitten in de software, in de programmatuur, maar ook in de systemen. Ook de cybersecurity die Microsoft bijvoorbeeld daaroverheen draait, gaat uiteindelijk out-of-date, en daarmee neemt het risico uiteindelijk wel toe. Aan de voorkant houden we daar rekening mee.

Wat onze werkplekken in relatie tot Microsoft betreft, hebben we niet de hele suite, want dan moet je alles openzetten. Dat is mooi, want dan heb je megatools en gaat het werk efficiënter, maar uiteindelijk is dat een stuk minder veilig. Dus daar houden we rekening mee. We zijn uiteindelijk ook niet afhankelijk van één aanbieder. Ik ken de interesse van mevrouw Kathmann. Ik volg haar zeker op het gebied van cloud en digitale

soevereiniteit. Ik ken ook haar initiatiefnota; volgens mij heet die Donkere wolken. Defensie kijkt ook naar een multicloud- en hybridecloudconstruct. Je ziet dat we daar zowel een cloud voor hooggerubriceerde informatie als een private cloud, maar ook een aantal landing zones hebben, want af en toe wil je wel de maximale capaciteit en leverage van zo'n provider kunnen gebruiken. Maar wij gaan altijd over onze eigen data, wij gaan altijd over welke applicaties we waar en wanneer aanzetten. We hebben ook genoeg technische controls om daar rekening mee te houden.

Daarmee denk ik dat ik er zo goed als doorheen ben. Dan wil ik nog een paar afsluitende opmerkingen maken.

De **voorzitter**:
Er zijn vragen naar aanleiding van dit mapje. De heer Pool, voor uw laatste interruptie ook.

De heer **Pool** (PVV):
Dank u wel, en u begrijpt dat ik daar heerlijk de tijd voor neem.

De **voorzitter**:
Dan weet u ook dat ik u ga afkappen.

De heer **Pool** (PVV):
Ik merk een disbalans tussen de Kamer en de staatssecretaris. Ik heb meerdere collega's gehoord die de staatssecretaris vroegen waarom hij zo lang wacht met het vitaal verklaren van dit belangrijke krijgsmachtsnetwerk. Maar de staatssecretaris zegt net in de beantwoording: ik wacht nog echt dat onderzoek af, en dan kijk ik wel. Plus: het kan ook nadelen hebben, want eigenlijk — ik chargeer even — gaan meer mensen zich hiermee bemoeien en dat maakt het wellicht lastiger voor Defensie. De NCTV zelf heeft natuurlijk al gewoon duidelijke stukken staan over ...

De **voorzitter**:
Wat is uw vraag? U zit namelijk echt aan uw tijd.

De heer **Pool** (PVV):
Ach, jeetje, u bent zo streng. De vraag is waarom de staatssecretaris de urgentie van de Kamer niet deelt. En het hoeft niet alleen maar nadelig te zijn als je het vitaal verklaart, want je krijgt ook hulp vanuit andere organisaties, bijvoorbeeld van de NCTV, met als doel dit netwerk weerbaarder te maken.

De **voorzitter**:
Dank voor uw vraag. De staatssecretaris.

Staatssecretaris **Tuinman**:
Ik denk dat de heer Pool en ik het wel met elkaar eens zijn en er hetzelfde over denken. De doelstelling van vitaal verklaren is dat het veilig is, dat je altijd kunt opereren, dat er een technische laag in zit, dat er een operationele gebruikerslaag in zit en dat er een strategische laag in zit, dus: hoe doe je dat uiteindelijk allemaal met je overheden? Dat is precies wat wij ook doen op dit moment. We zijn daadwerkelijk bezig met die fysieke veiligheidsmaatregelen op het gebied van de ARK. Daar hebben we het al over gehad. Ook zijn we bezig met die digitale veiligheidsmaatregelen door middel van de

oefeningen die we doen, of de stresstests of hoe je dat wilt noemen. En we zijn ook daadwerkelijk in gesprek over wie er nou allemaal op dat netwerk zitten. Dat staat ook in dat rapport. Is dat handig of niet, wat betekent dat? De heer Ellian maakt zich zorgen over de strategische afhankelijkheid van één partner of van je onderaannemers: daar zijn we dus ook mee bezig. We zijn dus wel degelijk met al die zaken bezig. Ik ga niet vooruitlopen op dat rapport, maar dat zijn wel allemaal zaken waar we op dit moment maatregelen op nemen.

Het klopt dat het goed is om met de NCTV samen te werken. We zijn ook daadwerkelijk aangesloten op het NCSC, het Nationaal Cyber Security Centrum. Sterker nog: met heel veel zaken doet Defensie ervaringen op, ook met dit soort netwerken, ook in de buitenwereld, ook met de lessen die we leren van Oekraïne. Daarmee voeden we uiteindelijk ook weer de NCTV. Dus we zijn wel degelijk aangesloten. Maar goed, u moet nog even wachten op dat rapport.

De **voorzitter**:
Ik kijk even de Kamerleden aan. Er zijn geen vragen meer met betrekking tot dit mapje. Dan kunt u de beantwoording van uw overige vragen doen.

Staatssecretaris **Tuinman**:
Voorzitter. Een andere kant, waar mevrouw Kathmann over sprak, vind ik ook wel mooi. Zij had het over trots. Ik vind dat wij in Nederland op sommige zaken ook wel wat trotser mogen zijn. Dat geeft verantwoordelijkheid. Ik ben best wel trots op dit netwerk, en ben nog veel trotser op de mensen die achter dit netwerk zitten. Ik vind ook dat het netwerk technisch betrouwbaar is. Dat onderschrijft de ARK ook. De fysieke beveiliging is een aandachtspunt; daar heeft u allemaal over gesproken. Ik werk daar ook hard aan. Een voorbeeld zijn de penetratietesten die ik doe. Mevrouw Kathmann had het ook nog over een bredere blik. Ze had het onder andere over AI-faciliteiten. Wat dat betreft vindt zij mij volledig aan haar zijde. Naar de toekomst toe heeft de krijgsmacht echt wel grote stappen gezet. We stoppen er veel geld in. We hebben er allerlei programma's op zitten, maar gelet op de conflicten die nu in de wereld plaatsvinden, moet de krijgsmacht klaar zijn, zodat het conflict of de oorlog uiteindelijk niet uitgevochten hoeft te worden. Daarin is digitalisering de next step. Dan gaat het erom hoe je ervoor zorgt dat je je data goed kunt bewerken. Dan gaat het over de cloud. Ook gaat het erom hoe je ervoor zorgt dat je daar goede modellen op kunt draaien en inzichten uit krijgt die een ander niet krijgt. Dat gaat dus over artificial intelligence en over kwantum. Dat is dus eigenlijk je CPU, je computing power. Als je die zaken bij elkaar brengt, dan levert dat een voordeel op voor de mannen en vrouwen van de krijgsmacht om de beste kans op succes te hebben. Ik denk ook dat dat nodig is voor Nederland, zeker ook qua dual use. Dus dat betekent ook iets voor onze concurrentiepositie. Dit kabinet is best enthousiast over de AI-faciliteit. Ik kijk daar ook naar. We moeten even kijken hoe dat er precies uit gaat zien. Ik zie voor Defensie wel toepassingen op dat gebied, niet alleen voor mijn eigen Nederlandse Defensie Academie, dus op het gebied van wetenschap, maar voornamelijk ook met als doel om te leren van alle data die verzameld wordt. Dan gaat het dus om de vraag hoe je je optreden moet aanpassen. Want het militaire optreden is echt veranderd door de toepassing van dit soort digitale faciliteiten. Maar ik zie misschien nog wel veel meer in de samenwerking met ons Nederlandse bedrijfsleven. Een van de aandachtspunten van minister Brekelmans is bijvoorbeeld drones. Drones zijn eigenlijk drie dingen: het is hardware, voornamelijk componenten; het is software, waar het hier over gaat; en het is hoe je uiteindelijk met je data omgaat. Daar heb je zo'n datafaciliteit voor nodig. Als je

dat goed hebt, dan leer je sneller dan tegenstanders. Dat is één. Het zorgt ervoor dat je weerbaarder bent en dat je verdediging op orde is, maar het zorgt er ook voor dat Nederland concurrerender wordt en dat we onze digitale standaard omhoog kunnen trekken. Ik denk echt dat het een win is op alle vlakken.

Daar wil ik het dan ook mee afsluiten, voorzitter.

De **voorzitter**:
Dank aan de staatssecretaris.

Staatssecretaris **Tuinman**:
In ieder geval mijn inbreng dan.

De **voorzitter**:
Ja. Dank aan de staatssecretaris voor de beantwoording van de vragen in de eerste termijn. Ik zie dat er geen vragen meer zijn. Ja, mevrouw Kathmann, u bent echt door uw …

Mevrouw **Kathmann** (GroenLinks-PvdA):
Het zijn vragen die niet beantwoord zijn.

De **voorzitter**:
O, excuus. Dat kan altijd. Als u een vraag heeft die nog niet beantwoord is, kunt u die altijd nog ter herinnering aan de staatssecretaris stellen.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Voorzitter, dank. Ik had twee specifieke vragen gesteld, even ter check of we nu echt op de goede weg zitten. Dat is: gebruikt u inmiddels een veiligere vorm van tijdsynchronisatie binnen het NAFIN? En zijn er inmiddels redundante back-upvoorzieningen ingericht voor tijdsignalen?

Staatssecretaris **Tuinman**:
Een goede technische vraag. We gebruiken al de veiligste vorm van tijdsynchronisatie die er in de markt is. We hebben de redundantie verder verhoogd. Als ik er nog dieper op inga, is het gerubriceerd, dus daar moeten we hier niet met elkaar over spreken. Maar goed, ik zit erbovenop. Ik begrijp echt wat u bedoelt. Nogmaals, we hebben echt een hele veilige vorm van tijdsynchronisatie. De redundantie in die klokken hebben we ook versterkt.

De **voorzitter**:
Volgens mij heeft u nu alle vragen beantwoord die zijn gesteld zijn in de eerste termijn. Dan ga ik naar de tweede termijn. Daarin hebben de leden één minuut spreektijd. Ik begin met de heer Pool.

De heer **Pool** (PVV):
Dank u wel, voorzitter. Hartelijk dank aan de staatssecretaris voor de beantwoording in de eerste termijn. De PVV heeft in de inbreng natuurlijk de nadruk gelegd op het belang van NAFIN, maar dat belang wordt hier in de hele Kamer gedeeld, en ook door de staatssecretaris. Dat is een belangrijke conclusie. Dat is ook goed. De PVV heeft er ook alle vertrouwen in dat de staatssecretaris hard werkt om dit netwerk veilig en

toekomstbestendig te maken. Wat wel jammer is, is dat de staatssecretaris niet kan toezeggen dat zo'n storing niet langer dan vier uur gaat duren, dus daar blijven we echt op drukken als PVV. Het is wel heel mooi dat hij echt kan uitsluiten dat er nu iemand zonder toegang op plekken komt waar hij niet zou moeten komen. Dat is dus mooi.

Tot slot. We hadden het net over de urgentie. De Kamer zit echt te drukken op: waarom moeten we nog maanden onderzoeken of het vitaal is? Waarom doen we het niet gewoon? Bij dezen dus nog de oproep: merk het aan als vitale infrastructuur en zorg dat al die facetten, bijvoorbeeld de NCTV, samenwerken om dit veilig te houden. Natuurlijk blijft Defensie dan de regie daarop houden, maar dit is zo belangrijk dat we daar niet nog maanden mee kunnen wachten.

Dank u wel, voorzitter.

De **voorzitter**:
Dank aan de heer Pool. Ik heb u wel een aantal seconden extra tijd gegeven, omdat u in de eerste ronde keurig binnen de tijd was. Nu is het woord aan mevrouw Kathmann.

Mevrouw **Kathmann** (GroenLinks-PvdA):
Voorzitter. In mijn eerste termijn vroeg ik ook om een toekomstvisie. Welke rol speelt het NAFIN nou over vijf jaar of over tien jaar? Ik krijg een beetje de indruk, zeg ik via de voorzitter, dat dat nog niet helemaal duidelijk is. Daarom is ook dat onderzoek of het vitaal moet zijn en of dat nou handig in die toekomstvisie. Ik denk dat bij die toekomstvisie ook hoort — ik ben heel blij dat de staatssecretaris die handschoen wil oppakken — dat er überhaupt een bredere rol ligt voor Defensie bij de bemoeienis met de digitale infrastructuur van Nederland. Daarom wil ik graag een tweeminutendebat aanvragen, want bij dit kabinet is het toch altijd nodig om dat met een motie te bekrachtigen, omdat de coördinatie op dit terrein soms een beetje mist.

De **voorzitter**:
Dank aan mevrouw Kathmann. We hebben de tweeminutendebataanvraag genoteerd. Dan gaan we over naar mevrouw Heite. Ik zeg wel dat ik u strikt aan uw één minuut ga houden, omdat u in de eerste termijn over uw tijd was. Mevrouw Heite.

Mevrouw **Heite** (NSC):
Dank u wel. Ik sluit me weer van harte aan bij mijn voorganger, net als in de eerste termijn. Ik heb nog één vraag. Die is wellicht al beantwoord, maar het is mij in ieder geval ontgaan. Dat is de vraag of er voldoende zicht is op welke vitale infrastructuren ook gebruikmaken van NAFIN, zoals andere gekoppelde civiele locaties, en of de staatssecretaris rekening houdt met een grootschalige uitbreiding van Defensie in de nabije toekomst. Ik heb dat nog niet helemaal scherp.

Dank u wel.

De **voorzitter**:
Dat was keurig binnen de tijd, mevrouw Heite. Ik had niet eens zo streng hoeven te zijn door u aan te manen om binnen de tijd te blijven. Dan ga ik over naar de heer Ellian.

De heer **Ellian** (VVD):
Dank u wel, voorzitter. Uiteraard dank ik de staatssecretaris voor zijn beantwoording en

uiteraard ook zijn … Ik ben gewend om "ondersteuning" te zeggen, maar ik moet eraan wennen dat ik dat niet in die vorm tegen mensen zeg. Maar ik bedoel het niet verkeerd als ik "ondersteuning" zeg; het is de gebruikelijke manier van spreken. Het is fijn dat we op deze manier van gedachten hebben kunnen wisselen over de toekomst van NAFIN. Ik bemerk wel dat de stip op de horizon me nog niet helemaal duidelijk is. Misschien kan de staatssecretaris daar nog iets over zeggen. Maar ik voel urgentie en ik zie dat er ook heel veel gedaan is. Het is fijn dat we kunnen uitsluiten dat onbevoegden toegang kunnen krijgen. Dat levert dit dan weer op. Ik heb wel zorgen over de onderaannemers. Op papier kun je het mooi inrichten, maar als er iets fout gaat, zijn we toch wel heel erg kwetsbaar. Ik ben uiteraard geïnteresseerd in de motie die mogelijk komt.

De **voorzitter**:
Dank aan de heer Ellian voor zijn inbreng. Dan ga ik over naar de staatssecretaris voor zijn tweede termijn.

Staatssecretaris **Tuinman**:
Voorzitter. Allereerst dank aan de commissie voor dit goede, inhoudelijke debat. Ik heb er ook wat aan gehad. Ik heb uw visie en punten meegenomen. Ik loop de vragen even langs.

De vraag van de heer Pool. We streven er altijd naar om het binnen vier uur te doen. We hebben maatregelen genomen waardoor het ook veel aannemelijker wordt dat we dat halen. Ik had aan u toegezegd dat mensen niet zomaar toegang kunnen krijgen. We doen er natuurlijk alles aan om dat verder te verbeteren.

U had het ook nog over het vitaal zijn. Ik wil daar nogmaals het volgende over zeggen. Het belang van het NAFIN-netwerk en hoe cruciaal en essentieel dat is — daarmee is het voor mij en voor dit kabinet vitaal — doet niks af aan het feit dat je het vitaal verklaart. Als je het vitaal verklaart, betekent dat namelijk dat ik met meer mensen allerlei zaken moet gaan doen en mogelijk … Maar goed, dat gaat het onderzoek uitwijzen. Daadwerkelijk vraagt u twee dingen van mij. Het moet een militair netwerk blijven en ik moet ervoor zorgen dat dit daadwerkelijk die militaire doeleinden faciliteert. Anderzijds krijg ik uit onderzoeken ook terug dat je in een crisis gewoon daadkracht moet hebben. Je moet direct kunnen ingrijpen en daar moet je de ruimte voor hebben. Daar gaat het onderzoek over en daar ga ik op terugkomen.

Mevrouw Kathmann, meneer Ellian en mevrouw Heite — eigenlijk vroeg u hier allemaal naar — vroegen mij: wat is de toekomstvisie dan? Voor mij is die zo helder dat ik daar eigenlijk te weinig tijd aan heb besteed. Het systeem bestaat nu al 26 of 27 jaar. We updaten dat regelmatig. We hadden de eerste versie van NTN en we gaan nu naar NTNv2. Dat betekent dat het sneller en beter wordt en dat kwetsbaarheden eruit worden gehaald. Daar zijn we de afgelopen twee jaar mee bezig geweest. Eind dit jaar of volgend jaar wordt dat afgerond. Dan is het systeem echt weer het meest up-to-date. Ik weet niet wie dit 26 of 27 jaar geleden bedacht heeft, maar diegene had wel een gouden idee en gouden handjes. De afgelopen twee jaar is bij veel mensen in de straat glasvezel aangelegd, maar dit netwerk ligt er dus al 26 jaar. Dit is robuuste glasvezel en dat gaat ook niet zo snel kapot, tenzij je er met gravertje doorheen graaft. Maar goed, dat kunnen we weer mooi detecteren. NAFIN is dus een cruciaal netwerk voor de krijgsmacht, waar we zeker nog een keer de levensduur mee aan de slag gaan. We blijven er dus in investeren, we blijven het gebruiken en we blijven het beter maken. We

zorgen dat het technisch veilig is, dat het robuust is en dat het een betrouwbaar datatransportnetwerk is. Misschien doelt u er ook op dat de krijgsmacht ook exponentieel aan het groeien is. Misschien wordt deze wel twee of drie zo groot als nu. Het mooie van zo'n glasvezelnetwerk is dat er zat ruimte is om dat daadwerkelijk uit te kunnen breiden. NAFIN blijft dus een cruciaal onderdeel van onze digitale infrastructuur, zeker voor de komende tien, vijftien, twintig jaar.

Dan had mevrouw Heite nog een vraag. Even kijken, hoor. Ik kan mijn eigen aantekeningen niet eens lezen. Zij vroeg of er voldoende gebeurd is …

De **voorzitter**:
Zal ik de staatssecretaris helpen en vragen of mevrouw Heite haar vraag kan herhalen?

Staatssecretaris **Tuinman**:
Ja, alstublieft.

De **voorzitter**:
Mevrouw Heite, kan u uw vraag kort herhalen?

Mevrouw **Heite** (NSC):
Ik heb nog een vraag waarvan ik niet helemaal zeker weet of die beantwoord is. Dat is de vraag of er voldoende zicht is op welke andere vitale infrastructuren gebruikmaken van NAFIN, zoals andere gekoppelde civiele locaties, en of de staatssecretaris ook rekening houdt met de grootschalige uitbreiding die ophanden is.

Staatssecretaris **Tuinman**:
Op het tweede deel heb ik natuurlijk antwoord gegeven. Als we iets uitbreiden, er een locatie bij komt, dan wordt daar standaard een loopje voor dat netwerk bij gelegd. Dat doen we dus sowieso. De ruimte op het netwerk is qua capaciteit zeker voldoende voor de groei in de komende jaren. En we weten precies welke instellingen en locaties hieraan vastzitten. Dat ga ik niet delen, want dat hoeft niet iedereen te weten. Maar we weten precies welke aansluitingen we hebben op onze militaire locaties en welke er civiel zijn. Daar zitten we bovenop.

De **voorzitter**:
Dank. O, excuses.

Staatssecretaris **Tuinman**:
Dan had meneer Ellian nog een opmerking over de onderaannemers. Die zorg deel ik met de heer Ellian. Dat geldt niet alleen voor dit netwerk; dat geldt eigenlijk voor elk ecosysteem waar we mee bezig zijn. Daarom zijn we in het kabinet ook met weerbaarheid aan de slag. Daar zitten een aantal zaken in, bijvoorbeeld een weerbare economie, waar we de zes weerbaarheidslijnen hebben. We komen binnenkort als kabinet met de hoe-brief, waarin staat hoe we dat doen. Daarnaast zit onze MIVD er ook bovenop. Zeker daar waar ze cruciale aspecten in hebben, zitten we erbovenop, ook wat betreft de kwestie of mensen de juiste certificering hebben. We hebben natuurlijk ook een heel team — daar zeg ik niet te veel over, maar dat weet de heer Ellian wel — dat kijkt naar economische veiligheid, industrie en dat soort zaken. Uw zorg is dus ook mijn zorg. Dat is ook de zorg van de heren links en rechts naast mij.

De **voorzitter**:
Dank voor de beantwoording van de staatssecretaris in de tweede termijn. We hadden twee collega's die door hun interrupties waren, maar gezien de tijd en omdat een collega vroeg om een extra interruptie, sta ik een extra interruptie toe voor die twee collega's. De andere collega's hebben nog interrupties over. De heer Pool wil nog een korte interruptie plegen.

De heer **Pool** (PVV):
Dank u wel, voorzitter. U bent ruimhartig vandaag.

Over het aanwijzen van de vitale infrastructuur. Deze staatssecretaris heeft het altijd over de "whole of society"-benadering. Die is belangrijk. Maar als het hierom gaat, houdt hij andere partners het liefst zo ver mogelijk bij zich vandaan, omdat dat bemoeienis zou kunnen opleveren. Ik zou toch echt willen vragen om er iets positiever naar te kijken, want ook bijvoorbeeld de veiligheidsregio's kunnen heel goed ondersteuning bieden als iets als vitale infrastructuur is aangemerkt. Ik zou de staatssecretaris dus willen vragen om dat perspectief ook mee te nemen in het onderzoek dat loopt.

Staatssecretaris **Tuinman**:
Als de heer Pool mij vraagt om een positieve houding, dan neem ik dat ter harte en dan zal ik hier met een positieve houding naar kijken en zorgen dat we de suggestie die hij doet, serieus meenemen.

De **voorzitter**:
Dank. Ik kijk mijn collega's aan. Ik zie dat er geen vragen meer zijn. Dan dank ik de staatssecretaris en zijn ondersteuning voor de beantwoording van de vragen. Mag ik de staatssecretaris ook zeggen dat ik echt onder de indruk ben van zijn technische kennis? Dank daarvoor. Dank aan de Kamerleden voor hun inbreng, en dank aan eenieder, vooral de bode en de griffier voor de ondersteuning.

Dan sluit ik ... O, voordat ik de vergadering inderdaad sluit, het volgende. Er is een tweeminutendebat aangevraagd door mevrouw Kathmann. Dat zullen we doorgeleiden naar de Griffie plenair. Dan zal dat tweeminutendebat ingepland worden. Ik dank eenieder en sluit hierbij de vergadering.

Sluiting 11.51 uur.