Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 592 Defensienota 2024 – Sterk, slim en samen

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 59

VERSLAG VAN EEN COMMISSIEDEBAT

Vastgesteld 2 maart 2026

De vaste commissie voor Defensie en de vaste commissie voor Digitale Zaken hebben op 28 januari 2026 overleg gevoerd met de heer Brekelmans, Minister van Defensie, en de heer Tuinman, Staatssecretaris van Defensie, over:

- **de brief van de Minister van Defensie d.d. 3 oktober 2025 inzake Defensie Cyberstrategie (Kamerstuk 26 643, nr. 1422);**
- **de brief van de Staatssecretaris van Defensie d.d. 27 oktober 2025 inzake IT-portfoliostrategie (Kamerstuk 36 592, nr. 53);**
- **de brief van de Minister van Defensie d.d. 15 december 2025 inzake stand van zaken internationale inzet voor verantwoorde kunstmatige intelligentie in het militaire domein (Kamerstuk 33 694, nr. 71).**

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

De fungerend voorzitter van de vaste commissie voor Defensie,
Paternotte

De fungerend voorzitter van de vaste commissie voor Digitale Zaken,Kathmann

De griffier van de vaste commissie voor Defensie,
De Lange

kst-36592-59
ISSN 0921 - 7371
's-Gravenhage 2026

Voorzitter: Belhirch
Griffier: De Lange

Aanwezig zijn zes leden der Kamer, te weten: Belhirch, Boon, Van Duijvenvoorde, Erkens, Van Lanschot en Nanninga,

en de heer Brekelmans, Minister van Defensie, en de heer Tuinman, Staatssecretaris van Defensie.

Aanvang 10.32 uur.

De **voorzitter**:
Goedemorgen allemaal. Ik heet de bewindspersonen, hun ondersteunende ambtenaren en de collega's welkom. Voor vandaag hebben we het debat over de cyberveiligheidsstrategie van Defensie. De spreektijd is vier minuten. Ik stel voor dat we in de eerste termijn ieder vier interrupties geven. Het is wel de bedoeling dat het om een vraag gaat, en graag kort. Dan geef ik het woord aan de heer Van Lanschot.

De heer **Van Lanschot** (CDA):
Dank, voorzitter. De wereld verandert razendsnel en het strijdtoneel verandert mee. Onze digitale infrastructuur is het nieuwe front geworden. Cyberdreiging is reëel, constant en groeiend. De strategie spreekt van een permanente en proactieve inzet, waarbij Defensie niet alleen maar reageert, maar ook, terecht, offensiever durft op te treden. Het Defensie Cyber Commando, dat opgericht is voor de uitvoering van offensieve cyberoperaties, bestaat zo'n tien jaar. Wetgeving staat de zelfstandige uitvoering van operaties echter toch nog steeds in de weg. Daarom vraag ik het kabinet: is het, gelet op de voorgenomen wetswijzigingen, zoals de Wet op de defensiegereedheid, aannemelijk dat DCC in de nabije toekomst op eigen kracht offensieve cyberoperaties kan en mag voorbereiden en uitvoeren? Zo niet, hoe kunnen we dat dan regelen?
Voorzitter. De drie hoofdtaken in de strategie – eigen cyberveiligheid, militaire cyberoperaties en versterken van de cyberweerbaarheid van bondgenoten – bieden een heldere koers. Het CDA ziet graag dat de concrete uitvoering van deze taken regelmatig met de Kamer gedeeld wordt. Wij vragen ons af hoe Defensie in NAVO-verband gaat oefenen met cybercapaciteiten en hoe ook interoperabiliteit wordt geborgd.
Voorzitter. Zoals u weet, staat of valt iedere strategie met goed personeel. Zonder voldoende goed opgeleid personeel zijn ambities slechts van papier. Nu wordt er aangegeven dat er een innovatief wervings- en hr-beleid gevoerd gaat worden. Toch blijkt uit de informatie vanuit de praktijk dat de uitstroom nog steeds onverminderd hoog is. Kan de Minister of de Staatssecretaris aangeven waarom zij denken dat de genoemde maatregelen in het cyberdomein wel gaan werken of beter gaan werken dan bij de overige eenheden? Kunnen zij een indicatie geven van de redenen van de uitstroom?
Voorzitter. De Minister schrijft dat Nederland vooroploopt in de internationale dialoog over verantwoord gebruik van AI in het militaire domein. Het CDA wil het kabinet graag aanmoedigen deze kar te blijven trekken, maar AI mag wat ons betreft nooit het menselijke oordeelsvermogen volledig vervangen, zeker niet als het gaat om leven en dood. Kan de Minister aangeven hoe het gebruik van AI binnen Defensie wordt gemonitord en wordt getoetst aan het humanitair oorlogsrecht? Hoe wordt kennisdeling met bondgenoten en partners georganiseerd? Kan de Minister ook aangeven wat de invloed is van het feit dat Kyndryl als bedrijf met Amerikaanse wortels de nieuwe omgeving van Defensie ontwikkelt en in de toekomst deels gaat beheren?
Voorzitter, tot slot. Om innovatie te versterken heeft Defensie een programmadirectie Industrie en Innovatie opgezet en is er een budget

voor kortcyclisch inkopen. Allemaal goed nieuws. Maar helaas bereiken onze fractie signalen dat er ondanks de concrete vraag van een operationele eenheid om ook deze zomer op oefening het proven concept van een betrouwbaar consortium in de praktijk toe te gaan passen, de inkooptijdslijnen nog steeds te lang zijn om dit toe te staan. Herkent het kabinet deze signalen en, zo ja, hoe reflecteert het hierop?
Dank u wel.

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

De heer **Erkens** (VVD):
Dank u, voorzitter. Ik vervang vandaag collega Ellian, die een dubbele boeking had in het debatschema.
Voorzitter. De wereld is veranderd. In deze wereld zien we steeds meer digitale dreigingen vanuit landen zoals Rusland en China. De verschuiving naar een permanente proactieve tegendruk, zoals het kabinet beoogt, is wat de VVD betreft dan ook noodzakelijk en onvermijdelijk. Graag zou ik de Minister ook willen complimenteren om deze ambities. We moeten namelijk niet wachten tot de schade is aangericht. Onze krijgsmacht moet ruimte hebben om vijandelijke activiteiten tijdig en proactief te kunnen verstoren. Achteroverleunen op cybergebied kunnen we ons als Nederland daarom niet permitteren.
Deze ambitie vergt wel een stevig en juridisch fundament. De VVD dringt dan ook aan op een spoedige behandeling van de Wet op de defensiegereedheid. De huidige wet gaat nog uit van een verouderd onderscheid tussen vrede en conflict, dat in een cyberdomein al langer niet opgaat. Daarom vraag ik de Minister of het wetsvoorstel wel ver genoeg gaat om daadwerkelijk afschrikking te realiseren in het hybride domein. Gaan wij hiermee echt het verschil maken of behouden landen als China en de VS een grotere vrijheid van handelen? Ook vraag ik de Minister waar de resterende handelingsvrijheid van onze concurrenten precies vandaan komt en hoe hij borgt dat Nederland niet met één hand op de rug dit gevecht blijft vechten.
Een goede organisatie van het cyberdomein is ontzettend belangrijk voor de veiligheid van ons land. Daarom pleit de VVD voor een strakke regie om versnippering te voorkomen. Het is essentieel dat de DCS naadloos aansluit op de nationale en internationale cybersecuritystrategieën. Samenwerkingen tussen de MIVD, de NCTV en de politie moeten bij hybride dreigingen optimaal geborgd zijn. Hoe is de Minister van plan om die integrale aansturing te versterken? Waar is de regie belegd wanneer een incident zowel civiele als militaire raakvlakken heeft?
De VVD ziet een directe koppeling tussen personeelsbeleid en gevechtskracht. De voorspelbaarheid van projecten is significant gestegen, maar nog steeds pleit ik voor een flexibele schil in ons personeelsbestand. Graag zou ik willen dat Defensie creatiever kijkt naar flexibele salarisschalen. Daarnaast is het belangrijk dat we met de inzet van cyberreservisten toptalent aantrekken. Hoe ziet de Minister dit voor zich?
Voorzitter. Tot slot maak ik mij zorgen over onze houding ten opzichte van AI. Wat de VVD betreft is focus op menselijke controle prijzenswaardig, maar tegelijkertijd moeten we waken voor naïviteit. Oekraïne laat zien dat zowel de Russen als de Oekraïners op dit moment AI inzetten voor de eindfasegeleiding van zwerfmunitie, om zo elektronische verstoring te omzeilen. Dat is een trend die zich ook onmiskenbaar beweegt richting verdere automatisering, van doelselectie en ook besluitvorming op het slagveld. Europese technologische voorlopers, zoals het Duitse bedrijf Helsing, waarschuwen dat autonome zwermcapaciteiten die beslissingen kunnen nemen met een snelheid die de mens nooit kan bijbenen, binnen enkele maanden mogelijk al realiteit zijn. Graag vraag ik de Minister of we onze eigen bedrijven niet onnodig beperken in deze innovaties, die

immers al plaatsvinden op andere plekken op de wereld, en aangezien landen als Rusland zich hier zeker niet door laten remmen. Hoe borgen we dat de technologische voorhoede in Europa blijft en we niet onze relevantie verliezen aan landen die wat dat betreft met minder strenge kaders werken? Kunnen we het ons permitteren om inderdaad achter te blijven door onze bedrijven van deze beperkingen te voorzien? Wat de VVD betreft blijven we waakzaam, maar is er wel een stimulans nodig voor technologische vooruitgang op dit vlak, juist om ons land veilig te houden.
Dank u wel.

De **voorzitter**:
Dank u wel. De heer Boon, aan u het woord.

De heer **Boon** (PVV):
Voorzitter, dank u wel. De volgende oorlog zal beginnen met een paar toetsaanslagen vanachter een scherm. Geen waarschuwing, geen frontlinie, maar directe ontwrichting van vitale infrastructuur, militaire systemen en besluitvorming. Dat maakt het cyberdomein tot een van de meest kwetsbare en tegelijk meest onderschatte veiligheidsdomeinen. De Defensie Cyberstrategie 2025 laat zien dat het kabinet cyber expliciet als militair domein beschouwt. Voor de PVV is de vraag niet of dat nodig is, maar hoe deze koers zich vertaalt naar de praktijk. De strategie spreekt over een permanente proactieve cyberinzet. Kan de Minister concreet toelichten wat dit in de praktijk betekent? In dat kader is er ook de vraag hoe eenduidige militaire leiding in het cyberdomein wordt vormgegeven. Cyber raakt meerdere onderdelen binnen Defensie. Hoe wordt gezorgd voor duidelijke aansturing, heldere verantwoordelijkheden en een overzichtelijke commandostructuur? De strategie benadrukt daarnaast de samenwerking met kritieke publieke en private partners. De PVV ziet het belang daarvan, maar stelt daarbij de vraag hoe wordt voorkomen dat de Defensie door deze samenwerking afhankelijk wordt van partijen waarover zij geen volledige controle heeft, juist als het gaat om gevoelige informatie en operationele veiligheid, en of hierbij een voorkeur geldt voor samenwerking met Nederlandse bedrijven en onderzoeksinstituten. Een ander belangrijk aandachtspunt is personeel; dat is al eerder genoemd. Hoe maakt Defensie zich concreet een aantrekkelijke werkgever voor cyberspecialisten in een zeer competitieve arbeidsmarkt? Daarnaast vragen wij of er in de huidige opleidingen voor alle militairen voldoende aandacht is voor cyberveiligheid en het functioneren in het digitale domein, juist voor de militairen buiten de specifieke cyberfuncties.
Ook heeft de PVV een vraag over de toekomstige technologische ontwikkelingen. Wordt in de huidige Cyberstrategie expliciet rekening gehouden met de komst van de kwantumcomputer en de gevolgen daarvan voor encryptie, communicatiebeveiliging en militaire systemen? Verder zien we meerdere cyberstrategieën en weerbaarheidsvisies naast elkaar bestaan. Waarom is hiervoor gekozen? Is overwogen om deze te integreren tot één samenhangende strategie, met duidelijke regie en verantwoordelijkheid?
Voorzitter, mijn laatste vraag. Waar staat Nederland op dit moment in het cyberdomein ten opzichte van andere landen? Ziet de Minister signalen dat Nederland terrein wint, stagneert of juist achterop dreigt te raken?
Voorzitter, tot zover.

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

Mevrouw **Nanninga** (JA21):
Dank u wel, voorzitter. De fractie van JA21 is heel blij met de duidelijke bewustwording die uit dit Cyberstrategiestuk blijkt. Defensie erkent dat

het cyberdomein geen bijzaak meer is, maar een volwaardig operationeel domein. Ook de offensievere houding juichen wij toe. De analogie van de Minister snijdt ook hout: hoger druk zetten en verder van de eigen goal verdedigen. Dat heb ik me laten uitleggen door een medewerker; ik weet niets van voetbal. Maar hij zei dat dat een mooie analogie is, dus dat nemen we aan.
In het cyberdomein betekent dat: dreigingen eerder onderkennen, eerder verstoren en niet pas reageren als de schade al is aangericht. Dat is logisch, realistisch en nodig. Tegelijkertijd willen wij wel weten of dit meer is dan een heel overtuigend verhaal. De tekst is prima, maar cybercapaciteit ontstaat niet vanzelf. Die groeit niet aan een boom. Daarom hebben wij een aantal concrete vragen aan de Minister. Misschien is er enige doublure met de sprekers voor mij, maar goed.
Allereerst over mensen. Hoeveel extra fte wil Defensie specifiek aantrekken voor deze Cyberstrategie? Is daar een concrete raming van of blijft het bij de constatering dat – ik citeer – «voldoende gekwalificeerd personeel belangrijk is»? «Voldoende» is een beetje een vage term. In welk tijdsframe denkt de Staatssecretaris deze mensen daadwerkelijk binnen te hebben, gezien de krapte op de arbeidsmarkt en de stevige concurrentie met het bedrijfsleven, zoals ook al is genoemd?
Dan het geld. Hoeveel extra budget is er concreet nodig om deze strategie uit te voeren? Is daar al serieus over nagedacht? Komt dit nog in de reguliere planningscyclus? Zie ik een stuk over het hoofd waar dat al in staat? Dat kan natuurlijk ook. Als er extra middelen nodig zijn, wanneer verwacht de Minister hierover dan duidelijkheid te kunnen geven aan de Kamer? Dan gaat het zowel over de termijn als over een raming van het bedrag. Daarbij hebben wij ook de vraag of Defensie met de huidige capaciteit al een groot deel van deze strategie kan uitvoeren. Nederland behoort internationaal tot de top als het gaat om cybercapaciteiten. Wat kan er vandaag al en wat kan er echt nog niet zonder aanvullende investeringen? Waar zit dan de bottleneck?
Tot slot het juridisch kader. Welke wetgeving is nodig om deze strategie volledig te kunnen uitvoeren? Waar knelt het op dit moment in bevoegdheden of kaders? Is er al wetgeving in voorbereiding en, zo ja, is die al ergens te vinden? Hoeveel spoed heeft dit wat de Minister betreft, gezien het feit dat cyberdreigingen zich helaas niet keurig aan onze wetgevingstrajecten houden?
Tot zover onze vragen, voorzitter. Dank u wel.

De **voorzitter**:
Dank u wel. Dan nodig ik u uit, meneer Van Duijvenbode. Van Duijvenvoorde. Mijn excuses.

De heer **Van Duijvenvoorde** (FVD):
Geen probleem.
Voorzitter. Ik heb ook een aantal vragen die al gesteld zijn, maar dan zullen we maar zeggen dat dat de belangrijke vragen zijn om te beantwoorden.
Forum voor Democratie staat voor een sterk en onafhankelijk leger, een krijgsmacht die het Nederlandse grondgebied en onze belangen daadwerkelijk kan verdedigen. In die context is het terecht dat Defensie het cyberdomein beschouwd als een volwaardig operationeel domein. De nieuwe Defensie Cyberstrategie markeert echter een wezenlijke verschuiving van een reactieve naar een permanente, proactieve inzet, ook onder de drempel van gewapend conflict. Defensie spreekt expliciet over de «grijze zone», het gebied tussen vrede en oorlog.
Voorzitter. Als cyber permanent wordt ingezet, ook buiten formeel conflict, dan is dat geen technische, maar een politieke keuze. Mijn eerste vraag aan de Minister is daarom: hoe borgt hij dat deze permanente cyberinzet in de zogenoemde grijze zone daadwerkelijk defensief blijft en niet

ongemerkt overgaat in escalatie, zonder expliciete politieke besluitvorming? Waar ligt de grens en wie bewaakt deze grens?
Voorzitter. Een strategie staat of valt met mensen. Gespecialiseerd cyberpersoneel is schaars, terwijl Defensie fors wil opschalen. De Minister stelt dat de inzet van reservisten de druk op de arbeidsmarkt beperkt, omdat zij werkzaam blijven bij een civiele werkgever. Ik heb de Minister recent middels Kamervragen gevraagd hoe hij voorkomt dat deze ambitie leidt tot extra druk op een toch al krappe arbeidsmarkt. In zijn schriftelijke beantwoording stelt de Minister dat door de inzet van reservisten de gevolgen voor de arbeidsmarkt beperkt blijven, omdat zij werkzaam blijven bij hun reguliere werkgever. Die redenering vraagt enige nuancering. Ook reservisten kunnen hun tijd maar één keer inzetten. Elk uur dat een IT-specialist beschikbaar is voor Defensie, is een uur dat hij niet beschikbaar is voor het bedrijfsleven. Daarmee wordt ook via het reservistenmodel capaciteit onttrokken aan dezelfde schaarse arbeidsmarkt. Defensie en het bedrijfsleven zijn hier geen tegenpolen, maar wederzijds afhankelijk. Zonder een sterke economie kan Defensie niet worden bekostigd en zonder veiligheid kan de economie niet floreren. Daarom stel ik de Minister de volgende vragen. Erkent de Minister dat ook de inzet van cyberreservisten structureel druk legt op de arbeidsmarkt, omdat hun inzet voor Defensie ten koste gaat van de beschikbare arbeidscapaciteit in het bedrijfsleven? Hoe bewaakt de Minister deze wederzijdse afhankelijkheid concreet? Welke mechanismen hanteert hij om te voorkomen dat de versterking van Defensie leidt tot verstoring van vitale economische sectoren?
Voorzitter. Defensie erkent zelf dat het voor cyber- en AI-innovatie afhankelijk is van het bedrijfsleven; dat is realistisch. Tegelijkertijd zien we dat Nederland en de Europese Unie innovatie steeds zwaarder reguleren met normering, ethische kaders en de AI-verordening. Hier ontstaat een spanning. Terwijl Defensie afhankelijk is van private innovatie, wordt diezelfde private sector geconfronteerd met toenemende beperkingen. Mijn vraag aan de Minister is daarom hoe hij het streven naar militaire slagkracht rijmt met een beleid dat private AI-innovatie structureel afremt. Hoe kan Defensie afhankelijk zijn van private AI-ontwikkeling terwijl die sector door Europese en nationale regelgeving steeds verder wordt ingeperkt? Is de Minister bereid zich in Europees verband in te zetten voor meer ruimte binnen de AI-verordening van de EU, juist waar het gaat om veiligheid en defensie?
Voorzitter. Cyberstrategie draait uiteindelijk om keuzes: over politieke controle, over schaarse capaciteit en over de vraag of wij bereid zijn om de voorwaarden te scheppen voor de echte slagkracht. Daarom hoor ik graag een helder antwoord van de Minister op deze vragen. Dank u wel.

De **voorzitter**:
Dank u wel. U hebt een interruptie van de heer Van Lanschot.

De heer **Van Lanschot** (CDA):
Via u een vraag aan de heer Van Duijvenvoorde. Ik ben benieuwd hoe Forum voor Democratie denkt over de samenwerking in Europees verband op het gebied van cyber.

De heer **Van Duijvenvoorde** (FVD):
Het is nu eenmaal zo dat Defensie op dit moment Europees opereert. We kunnen er een hele discussie over voeren wat FVD daarvan vindt; maar binnen deze context, waarin we toch al samenwerken, geloven wij dat we cyber ook met elkaar moeten aanpakken. Of we uiteindelijk voor een Europese samenwerking zijn, is een ander debat.

De **voorzitter**:

Dan wil ik graag het voorzitterschap overdragen aan de heer Erkens, zodat ik mijn bijdrage kan doen.

Voorzitter: Erkens

De **voorzitter**:
En dan geef ik het woord aan mevrouw Belhirch van D66 voor haar inbreng.

Mevrouw **Belhirch** (D66):
Dank u wel, voorzitter. We zagen het allemaal: chaos op luchthavens in Berlijn en Brussel, huishoudens zonder stroom in Polen. Dit is geen ver-van-ons-bedshow. Dit waren geen technische storingen, dit waren digitale aanvallen met directe gevolgen voor het dagelijks leven. Dat Defensie cyberveiligheid prioriteit geeft, is noodzakelijk. Juist daarom wil ik de Minister en de Staatssecretaris complimenteren met hun inzet en hun cyberveiligheidsstrategie.
Cyberveiligheid van Defensie gaat niet alleen over militaire capaciteit. Een digitale aanval raakt kritieke infrastructuur: energie, zorg en communicatie. Mijn vraag is dan ook wie de regie heeft als cyberaanvallen Defensie overstijgen en de samenleving raken. De focus op statelijke actoren is terecht, maar de dreiging komt ook van niet-statelijke actoren. Zijn onze juridische en operationele kaders daar voldoende op ingericht?
Voorzitter. Cyberveiligheid is niet alleen technisch, maar ook geopolitiek. Het raakt direct onze nationale veiligheid en weerbaarheid. Samenwerking met bondgenoten en private partijen is nodig, maar samenwerking mag nooit blindheid worden voor afhankelijkheid en soevereiniteit. Niet voor niets is een meerderheid in deze Kamer voorstander van digitale soevereiniteit. Digitale soevereiniteit is geen ideologisch ideaal, maar een randvoorwaarde voor veiligheid in een wereld waarin data macht is. Dat wordt concreet bij Palantir, een bedrijf dat diep verweven is in het Amerikaanse overheidsapparaat. Dat biedt snelheid en operationeel voordeel, maar het wordt ook ingezet bij militaire operaties en bij binnenlandse handhaving, waaronder deportaties door ICE. Via dit soort systemen worden miljoenen privacygevoelige gegevens verwerkt. Het gaat niet alleen om technologie, maar ook om controle en afhankelijkheid. Daarom mijn vragen: wie is eigenaar van Nederlandse data en analyses die door bedrijven als Palantir worden verwerkt? Heeft de Minister zicht op kritieke afhankelijkheden en is er een exitstrategie als toegang tot onze data onder druk komt te staan?
Voorzitter. Ik ben positief over de stappen die Defensie en het bedrijfsleven zetten richting eigen technologie, om minder afhankelijk te worden van partijen buiten Nederland en Europa. Zo ver zijn we echter nog niet. Samenwerking met private partijen blijft nodig, maar vraagt om harde randvoorwaarden. Hoe borgen we nationale veiligheid bij ketenafhankelijkheden in publiek-private samenwerking? Welke eisen gelden voor cybersecurity, auditbaarheid en transparantie? In de Defensiestrategie staat dat bij aanbestedingen strenge eisen gelden. Mijn vraag is of daarin ook expliciet internationaal recht en mensenrechten zijn geborgd. Hoe weegt de Minister het gebruik van Palantir in het licht van onze ambities op het gebied van digitale soevereiniteit en mensenrechten?
Voorzitter. Het cyberdomein ontwikkelt zich razendsnel, terwijl Europese regelgeving achterblijft. Dat schuurt, maar biedt ook kansen. Nederland is een koploper en zou binnen Europa richting moeten geven. Welke stappen zet Nederland om die rol te pakken? Hoe bouwen we strategische afhankelijkheden van niet-Europese partijen af?
Voorzitter. Deze strategie is een juiste en noodzakelijke eerste stap. We moeten verder bouwen aan cyberveiligheid en weerbaarheid om onze nationale veiligheid en digitale soevereiniteit te versterken. Zo kan Nederland weerbaarder en richtinggevend zijn in Europa.

Dank u wel.

De **voorzitter**:
Ik zie geen interrupties. Ik draag het voorzitterschap weer aan u over.

Voorzitter: Belhirch

De **voorzitter**:
Dank u wel. Dan wil ik de vergadering graag schorsen tot 11.15 uur.

De vergadering wordt van 10.53 uur tot 11.15 uur geschorst.

De **voorzitter**:
Ik nodig de Minister uit voor zijn eerste termijn.

Minister **Brekelmans**:
Dank, voorzitter, en dank aan de leden voor alle goede vragen. Ik zal eerst even aangeven welke categorieën we hanteren. Ik begin met de Defensie Cyberstrategie en wat algemene vragen daaromtrent. Daarna zal ik in wat meer algemene zin stilstaan bij het thema soevereiniteit, waar meerdere vragen over zijn gesteld. Dan komt het kopje internationaal en internationale samenwerking. Daarna taken en verantwoordelijkheden, zowel binnen Defensie als daarbuiten. Dan wetgeving, waarover ook een aantal vragen zijn gesteld. Ik eindig met het onderwerp AI. De Staatssecretaris zal spreken over personeel. Hij zal ook specifieker ingaan op soevereiniteit en het afbouwen van specifieke afhankelijkheden. Hij zal iets zeggen over inkoop en over industrie. Ik sluit niet uit dat we allebei nog een categorie overig hebben, maar dit zijn de hoofdonderwerpen.
Voorzitter. Ik hoop dat u mij toestaat nog even iets algemeens te zeggen voordat ik begin en specifiek op cyber inga. De afgelopen dagen hebben de uitspraken van president Trump veel losgemaakt binnen Defensie en ook breder, binnen de veteranengemeenschap. Dat betrof in het bijzonder de opmerking dat militairen uit andere landen niet in de frontlinie zouden staan en niet bereid zouden zijn om daar verantwoordelijkheden in te dragen. Ik heb daar direct een reactie op gegeven in de media. Ik heb gezegd dat ik deze opmerkingen ongepast en ook incorrect vond.
Ik vind het ook belangrijk om hier, in het eerste debat dat ik daarna heb, in het hart van de democratie, nog iets daarover te zeggen. In de afgelopen anderhalf jaar dat ik Minister was, hebben juist de verhalen uit Afghanistan, over wat onze militairen en veteranen daar hebben meegemaakt, mij het meest gegrepen. We zitten hier met de Staatssecretaris, die uit eigen ervaring van alles kan vertellen over hoe onze militairen daar gevaar hebben gelopen en hun leven hebben geriskeerd, alles in de strijd tegen terrorisme, om ervoor te zorgen dat de mensen in Nederland en Europa, maar ook in de Verenigde Staten minder gevaar lopen als het gaat om terroristische dreigingen. De uitspraken die de Amerikaanse president daarover heeft gedaan, zijn apert onjuist en ook kwetsend. Ik vind het respectloos. Die uitspraken doen geen recht aan de belangrijke bijdrage die onze militairen daar hebben geleverd.
Aankomende maandag is het twintig jaar geleden dat het parlement de missie in Uruzgan heeft goedgekeurd. Wij hebben een breed mandaat gegeven, ook politiek, aan onze militairen en zij hebben daar gestreden voor onze vrijheid en veiligheid. Onze CDS heeft het heel mooi gezegd: onze militairen en veteranen verdienen geen ontkenning, maar erkenning voor wat er is gebeurd. Als Minister van Defensie zal ik er altijd voor staan dat we die erkenning geven en dat we onze waardering en eerbied uitspreken voor wat onze militairen voor ons hebben gedaan.
Ik vind het heel goed dat de Amerikaanse ambassadeur heeft gezegd dat de uitspraken van president Trump niet op Nederland van toepassing waren. Ik vind het ook goed dat de president in ieder geval voor de Britse

militairen zijn uitspraken heeft gecorrigeerd. Het zou hem sieren als hij dat breder zou doen en specifiek de Nederlandse militairen zou noemen. Tot het moment dat dat is gebeurd, zal ik in ieder geval bij de Amerikaanse regering steeds onder de aandacht brengen dat wij wel degelijk in de frontlinie hebben gestaan en onze verantwoordelijkheid hebben genomen. Ik vond het belangrijk om dat voorafgaand aan het debat in de Kamer te zeggen.

Dan ga ik over naar het onderwerp van het debat: cyber. Ik begin met de eerste categorie, namelijk met een aantal algemene opmerkingen over de Cyberstrategie. Een aantal leden hebben gevraagd naar de proactieve inzet, gericht op niet alleen defensieve, maar ook offensieve activiteiten. Dat is denk ik een van de grotere veranderingen in vergelijking met de Cyberstrategie van een aantal jaar geleden. Wij erkennen die noodzaak namelijk en benoemen die ook expliciet zo. Dat is deels, moet ik zeggen, ook al eerder in het debat met de Kamer ter sprake gekomen. We hebben het eerder over het onderwerp cyber gehad, voordat deze strategie er lag. Er was een duidelijke wens van meerdere fracties om te kijken of we hier als krijgsmacht offensiever in zouden kunnen opereren, gegeven alle dreigingen die op ons afkomen. Dat hebben wij ter harte genomen en verwerkt in de strategie.

Wat houdt dat dan concreet in? Dat houdt concreet in dat je zowel aan de contra-inlichtingenkant als aan de militaire kant iets hoger druk zet, zoals mevrouw Nanninga dat noemde. Dat betekent dat je mogelijke cyberdreigingen eerder probeert te onderkennen en daar mogelijk ook bepaalde posities voor inneemt, en dat je oefent en traint voor de militaire inzet van cybercapaciteit, zodat je in staat bent die toe te passen als dat nodig is. Een aantal leden benoemden dat het daadwerkelijk overgaan tot een cyberaanval, wat een groot effect zou hebben, wel een militaire activiteit is. Voordat je daartoe overgaat, hoort daar de gebruikelijke parlementaire besluitvorming bij zoals die bij iedere militaire activiteit nodig is. Over de inlichtingenkant en wat de MIVD en de AIVD daar precies in doen kan ik, zoals u weet, niet in het openbaar spreken. Daarover leggen we in de CIVD, de commissie voor de Inlichtingen- en Veiligheidsdiensten, aan de Kamer verantwoording af. Dat is niet iets waar we openlijk over spreken. Maar dat zijn dus manieren waarop we concrete invulling geven aan die meer offensieve inzet: dreigingen eerder onderkennen, in staat zijn om offensieve acties uit te voeren, en waar nodig al eerder posities innemen om die zaken te kunnen waarnemen. Daarbij gaan we dus niet de grens over naar een cyberaanval, wat als een militaire offensieve actie zou kunnen worden gezien. Voor zo'n actie is inderdaad een legitimiteit nodig en in sommige gevallen, afhankelijk van de context, is ook een mandaat vanuit de Kamer gewenst.

Dan was er een vraag over de strategie. Welke middelen zijn daarvoor nodig? Mevrouw Nanninga vroeg dat, maar anderen ook. Deze strategie is opgesteld binnen de huidige financiële kaders. Als dat niet zo was, zou het Ministerie van Financiën, en specifiek de Minister van Financiën, mij aan de kraag trekken om te zeggen dat we geen strategieën naar de Kamer sturen waar geen dekking voor is. Deze strategie is dus uitvoerbaar binnen de financiële kaders die we hebben. Natuurlijk zitten er in die strategie ook een aantal ambities verscholen, namelijk capaciteiten die we verder willen uitbouwen en verstevigen en waar we meer in willen investeren. De mate waarin we dat kunnen doen, zal natuurlijk ook afhangen van de financiële middelen die een nieuw kabinet daarvoor vrijmaakt. Wanneer we met een nieuw kabinet richting de 3,5% zouden gaan, wat zou leiden tot een hoger budget voor Defensie, zou een deel van deze strategie dus ook meteen vertaald zijn. Een deel van dat budget wordt namelijk ook gebruikt om te investeren in onze capaciteiten om ze verder te versterken en uit te breiden.

Hoeveel is dat dan concreet precies? Ik kan daar op dit moment geen geldbedrag aan hangen, zo van: dat is zoveel miljoen of miljard. We zullen

dat verder gaan uitwerken. Het is ook afhankelijk van de mate waarin het budget toeneemt en natuurlijk van hoe dat past binnen de bredere prioriteiten die we als Defensie hebben. Maar goed, zodra die budgettaire kaders beschikbaar zijn, is de wens natuurlijk om op relatief korte termijn verdere invulling te geven aan de uitwerking daarvan. We willen als Defensie namelijk volop doorgaan met zowel het laten groeien als het moderniseren van onze krijgsmacht.
Dan ga ik naar de tweede categorie, die hiermee samenhangt. Dat is soevereiniteit. Natuurlijk werken wij samen met private partners en maken wij ook gebruik van software en hardware die van private partners komen. Gegeven alle ontwikkelingen die er in de wereld zijn – leden hebben daar verschillende voorbeelden van genoemd – bekijken wij natuurlijk steeds kritischer of we voldoende soeverein zijn, of er geen kwetsbare afhankelijkheden zijn en, als die er wel zijn, in welke mate en met welke snelheid we in staat zijn om die af te bouwen. Vanuit Defensie zijn wij daar, denk ik, in vergelijking met heel veel andere organisaties, sowieso al voorzichtig in geweest, zou je kunnen zeggen. We hebben een eigen IT-organisatie die zorgt dat we ook zelf systemen en software beheren en dat we die afhankelijkheden beheersbaar houden. In specifieke contracten worden ook altijd elementen opgenomen die ervoor zorgen dat we niet tot het einde der tijden afhankelijk zijn van die leverancier, maar dat er ook altijd de mogelijkheid is om over te stappen op een ander of om het eventueel zelf te doen. We zorgen er ook voor dat we daar de kennis, de kunde en de capaciteit voor in huis houden.
Er zijn verder nog een aantal zaken die we specifiek doen. We kijken kritisch naar ons cloudbeleid en brengen daar verdere aanscherpingen in aan. De Staatssecretaris kan daar zo meteen in meer detail op ingaan. Bij onze IT-inkoop stellen we ook voorwaarden aan de leveranciers en de afhankelijkheden daarvan. We maken ook zo veel mogelijk gebruik van open standaarden, want dan kun je andere software of andere aanbieders daarop inklikken en ben je in staat om het eventueel ook zelf over te nemen. Dat vermindert dus de afhankelijkheid. En we investeren natuurlijk in onze eigen kennis en capaciteit, zodat we niet afhankelijk zijn van de kennis en expertise van een specifieke leverancier. Maar goed, de Staatssecretaris zal op de specifiekere vragen ingaan. Er zijn bijvoorbeeld vragen gesteld over Palantir. Daar zal de Staatssecretaris verder op ingaan.
Dan kreeg ik de vraag hoe we internationaal samenwerken. Op het gebied van cyber is de lijst samenwerkingsverbanden en samenwerkingsinitiatieven heel erg lang en breed. Ik zal die dus niet allemaal opnoemen. Binnen de NAVO voeren we ook gezamenlijk oefeningen uit, specifiek op het gebied van cyberveiligheid en cyberweerbaarheid. Zo nemen we jaarlijks deel aan de NAVO-oefeningen Locked Shields en Cyber Coalition, waarin dat soort zaken worden gedaan. Daarnaast maakt cyber ook van steeds meer NAVO-oefeningen een prominent onderdeel uit. Dus wat je dan oefent, is dat je aan de ene kant een fysiek effect bereikt of een fysiek scenario oefent, maar dat daar ook een cyberelement in verweven zit. Het is dus niet zo dat cyber altijd losstaat; je probeert dat natuurlijk zo veel mogelijk in een multidomeinoefening te verwerken.
Waar het gaat om samenwerking, proberen we ook om andere landen waarvan de cybercapaciteiten minder op orde zijn te helpen met training en ondersteuning. Die training en ondersteuning vinden deels via de NAVO plaats en ook via de EU. In sommige gevallen zijn die ook bilateraal. Verder kijken we ook in NAVO-verband naar hoe we de samenwerking tussen de cybereenheden van verschillende landen kunnen verbeteren. Er zijn ook verschillende mechanismen om ervoor te zorgen dat we elkaar niet in de weg zitten en dat we dat synchroniseren en afstemmen, zodat we daar ook meer gezamenlijk in kunnen opereren.
Dan had de heer Boon van de PVV nog de vraag waar Nederland nu in het cyberdomein staat ten opzichte van andere landen. Het is moeilijk om

daar een score aan te hangen – zo eenvoudig is het niet – maar over het algemeen kun je zeggen dat er een groep landen is die hierin vooroploopt en dat Nederland een van die landen is. We hebben specifieke dingen waar we sterk in zijn en er zijn ook dingen waar andere landen weer sterker in zijn, maar over het algemeen doen we goed mee, denk ik. Tegelijkertijd gaan de ontwikkelingen zo snel dat dat ook continue investeringen en natuurlijk continue aandacht vraagt; een vooraanstaande positie behoud je niet zomaar. Daarom heeft het opbouwen van kennis en vaardigheden en het aantrekken van mensen ook zo'n prominente plek in de strategie.
Voorzitter. Dan ga ik naar taken en verantwoordelijkheden. Binnen Defensie wordt er aangestuurd binnen de bestaande militaire lijnen. We hebben het CEMA-bataljon opgericht binnen de landmacht en dat opereert ook binnen de landmacht. Dat is juist omdat je, zoals ik net zei, multidomein wilt kunnen opereren. Je wilt dus in staat zijn om een bepaalde actie uit te voeren en het opereren via bijvoorbeeld het landdomein of via het luchtdomein mogelijk te maken door via een cyberaanval systemen van de tegenstander uit te schakelen of door de elektriciteit van de tegenstander uit te schakelen. Op die manier wordt er dus ook geopereerd. Het is volgens mij dus verstandig om niet alle eenheden in een soort van losse cyberkolom te laten maar om dat juist ook dicht bij de verschillende eenheden te organiseren. Natuurlijk werken we dwars daarop wel aan het versterken van onze cybercapaciteit, dus zodat die onderlinge samenwerking plaatsvindt. We hebben een ontzettend goede CIO die daar een belangrijke rol in vervult – we werken dus ook op die manier aan onze capaciteitsopbouw – zodat niet iedere eenheid of ieder team dat daarmee bezig is zelf het wiel moet uitvinden.
Wie heeft de regie als er een digitale aanval plaatsvindt en de kritieke infrastructuur onder druk staat? In eerste instantie zijn dat de NCTV en Justitie en Veiligheid, omdat de coördinatie op het gebied van cyberveiligheid daar ligt. Wanneer er sprake zou zijn van een cyberaanval die dusdanig zwaar is dat je zou kunnen spreken van een militaire daad en je zelfs aan artikel 5 zou kunnen denken, komen we in een ander scenario terecht en kunnen ook de rollen en verantwoordelijkheden veranderen, maar dan zit je in een militair conflict. Tot die tijd is het de NCTV die de coördinatie doet en de regie voert over de crisis en de mogelijke gevolgen daarvan. Wij als Defensie zijn natuurlijk nauw daarop aangehaakt en ondersteunen daarin waar nodig. We hebben onze Cyberstrategie in nauwe samenwerking met Justitie en Veiligheid en met andere partners opgesteld, zodat ook geldt dat de samenwerking tussen de verschillende ministeries en tussen de verschillende organisaties die zich met cyber bezighouden, voldoende op elkaar aansluit.
Dan nog een vraag over samenwerking. Het Defensie Cyber Commando werkt bijvoorbeeld nauw samen met de MIVD en ze werken ook in gezamenlijke teams. Dat leidt ertoe dat als de MIVD werkt onder de Wiv en bepaalde activiteiten daarin uitvoert, ook vanuit DCC ondersteuning kan worden geboden met de capaciteiten die zij hebben. Je ziet steeds vaker dat ook DCC daarin onder de vlag van de Wiv opereert.
Ik denk dat ik daarmee alle vragen heb beantwoord. Er is natuurlijk ook nog samenwerking met de private sector. Daarvoor geldt dat die in eerste instantie vooral ligt bij Justitie en Veiligheid als het gaat om de cyberweerbaarheid van bedrijven, banken en dergelijke. Maar ook daarin werken wij natuurlijk nauw met hen samen. Een onderliggende vraag is steeds hoeveel informatie je daarover met elkaar kunt delen, want soms zijn het onze diensten die een bepaalde dreiging zien en soms zijn het juist eerder financiële instellingen of andere organisaties die dat sneller zien. Je wil dat de samenwerking op dat moment goed is, zodat informatie snel wordt uitgewisseld.
Een discussie die we ook nog als onderdeel van de herziening van de Wiv zullen hebben, is in hoeverre je organisaties daartoe kunt verplichten. Ik

ben er zelf, zeg ik als voorschot, voorstander van om daar verdere stappen in te zetten, omdat onze tegenstanders op zoek gaan naar de meest zwakke plek. Als je dan afhankelijk bent van een gemeente of een andere organisatie die al dan niet bereid is om mee te werken, maakt dat je heel kwetsbaar. Ik denk dat het heel veel duidelijkheid kan bieden als je heel duidelijke regels opstelt over welke informatie in welke gevallen met de diensten gedeeld moet worden. Uiteindelijk komt dat onze veiligheid ten goede. Maar laten we dat vooral bij de herziening van de Wiv bespreken. Dat biedt een logisch bruggetje naar het kopje wetgeving. Verschillende leden vroegen in hoeverre de Wodg eraan gaat bijdragen dat we in staat zijn om te doen wat nodig is. De Wodg zal daar een belangrijke bijdrage aan leveren. Ik zeg er meteen bij dat die niet de oplossing is voor alles. Op dit moment ligt het wetsvoorstel bij de Raad van State. Zodra het terug is en we het advies hebben verwerkt, zal het uiteraard richting de Kamer gaan. Het huidige wetsvoorstel ziet er vooral op dat we als Defensie ook gebruik kunnen maken van opensource-informatie. Daar zitten op dit moment behoorlijk wat beperkingen in, terwijl er natuurlijk ontzettend veel opensource-informatie is die nuttig en bruikbaar is voor onze veiligheid. Dat moet natuurlijk allemaal goed worden ingekaderd. Het is niet zo dat we direct zomaar alles kunnen. Maar het zal een belangrijk onderdeel zijn van de Wodg dat we meer in staat zijn om die informatie te gebruiken. Verder is natuurlijk de herziening van de Wiv met betrekking tot toezicht en toetsing op de diensten heel belangrijk. Dat zijn inderdaad twee belangrijke wetgevingstrajecten.

In beginsel zijn de wettelijke bevoegdheden, even los van de twee dingen die herziening behoeven, in die zin op orde dat de Cyberstrategie die we nu hebben, uitvoerbaar is met de kaders die er zijn. Ik vind daarbij wel dat als we die wettelijke kaders hebben, we daar ook gebruik van moeten maken. We moeten ook bereid zijn om de ruimte die er is, zo goed mogelijk en waar nodig maximaal te benutten.

Dan was er ook nog een vraag over het internationaal recht. Daarvoor geldt dat de Cyberstrategie die we nu hebben past binnen de internationale wet- en regelgeving, de internationale juridische kaders en de Europese kaders die daarvoor gelden. Die hebben we daarvoor als uitgangspunt genomen.

Ik kom op mijn laatste categorie. Een belangrijke discussie is natuurlijk die over AI. Op dit moment is er geen specifieke internationale wet- en regelgeving op het gebied van AI in het militaire domein. Het is op dit moment ook niet zo dat wij onze bedrijven meer belemmeren of tegenhouden met specifieke wetgeving dan onze tegenstanders dat doen. De reden waarom wij als Nederland het initiatief hebben genomen om het thema AI in het militaire domein op de kaart te zetten, is dat je zou kunnen zeggen dat er nu geen sprake is van specifieke regels en wetgeving op dit terrein en je dus ook niet de mogelijkheid hebt om anderen daarop aan te spreken. We hebben het internationaal recht en het humanitair oorlogsrecht. Daar zitten algemene bepalingen in die ook van toepassing zijn op AI, maar we hebben niet specifiek met elkaar afgesproken wat we wel en niet acceptabel vinden.

Volgens mij was het de heer Van Lanschot die vroeg: «In hoeverre wil je nou nog menselijke betrokkenheid houden? Wil je een human in the loop hebben en op welke momenten?» Het is goed om eerst internationaal afspraken te maken over dat soort principes en hoe je die verder uitwerkt, zonder daarin naïef te zijn. We weten namelijk ook dat onze tegenstanders zich ongetwijfeld niet aan die afspraken zullen houden, maar dan heb je in ieder geval de mogelijkheid om anderen daarop aan te spreken en mogelijk vervolgens ook sancties en dat soort zaken op te leggen op het moment dat zij zich daar niet aan houden. Ik ben het zeer eens met wat de heer Erkens zei, namelijk dat we daarin realistisch moeten zijn. We moeten geen regels opleggen waarmee we onszelf te veel beperken ten opzichte van onze tegenstanders. Je ziet in die internationale discussie eigenlijk

twee uitersten. Je hebt landen die zeggen: AI is eng; laten we ons vooral heel erg beperken. En je hebt landen die zeggen: vrijheid, blijheid, sta alles maar toe. Wij proberen daarin een genuanceerde positie in te nemen: we moeten wel tot gemeenschappelijke kaders komen om anderen aan te spreken, maar die moeten ons niet zodanig in de weg zitten dat we gaan achterlopen op onze tegenstanders. Ik ben er wel trots op dat wij als Nederland de eerste waren die het REAIM-congres hebben georganiseerd. We zitten ook bij de vijf landen die hierin wereldwijd het voortouw nemen. We hebben daarvoor een VN-resolutie ingediend. Samen met Kenia? Nee, met Zuid-Korea. Dus we nemen daarin echt het voortouw en dat is volgens mij ook heel belangrijk.
Dat was het, voorzitter.

De **voorzitter**:
Dank u wel. Er is een interruptie van de heer Van Lanschot.

De heer **Van Lanschot** (CDA):
Om nog even de positie van het CDA te verhelderen: die is dus dat er een human in the loop moet zijn. Dat was dus geen vraag, maar een stelling. De vraag aan de Minister is: begrijp ik het goed dat hij pleit voor een Genève-achtige conventie voor het toepassen van AI?

Minister **Brekelmans**:
We moeten kijken hoe ver we komen. We zijn begonnen met het REAIM-congres in Den Haag. De tweede sessie is vervolgens in Zuid-Korea geweest. Daar was ik vorig jaar ook bij. Volgende week is de derde bijeenkomst in Spanje. Daar zal ik ook aan deelnemen. Daar wordt over die kaders gesproken. Dat heeft zich vertaald in een VN-resolutie die met overgrote meerderheid in de AVVN is aangenomen. Dat is dus heel mooi. Of zich dat ooit kan vertalen in verdere juridische raamwerken moeten we bezien. Zover zijn we op dit moment nog niet, maar het zou wel heel mooi zijn als het lukt om daarover verdere afspraken te maken.

De **voorzitter**:
Daar heb ik zelf een vraag over. U zegt dat er stappen zijn gezet. Heel mooi dat Nederland daar het voortouw in heeft genomen samen met Zuid-Korea. U zegt dat de tijdlijn niet helder is. Maar wordt er diplomatieke druk op gezet om wel tot iets komen? Ik zei zelf net ook al dat het allemaal razendsnel gaat. Wetgeving gaat langzaam. De realiteit is wel dat er ruimte moet zijn. Hoe gaat het met het tijdspad?

Minister **Brekelmans**:
Ja, ik vind zelf het feit dat we vorig jaar die VN-resolutie met grote meerderheid aangenomen hebben gekregen echt wel een belangrijke stap. De landen die hierin het voortouw nemen zijn geografisch verspreid: Zuid-Korea, Kenia, Singapore en Spanje spelen daarin een rol. We proberen dat met een groepje landen verder vooruit te brengen. Overigens is die groep veel breder dan dat. Natuurlijk zit daar de druk op, maar het is steeds ook weer een afweging: hoe maak je niet alleen voortgang, maar zorg je er ook voor dat je veel landen meekrijgt? Als je te hard gaat, haken er namelijk weer landen af. Dat is zonde. En hoe zorg je ervoor dat je met elkaar afspraken opstelt waarvan je weet dat ze daadwerkelijk iets voorstellen? Het is namelijk heel makkelijk om met een groepje vooruitstrevende landen iets op papier te zetten waarvan je weet dat de spelers die er echt toe doen er verder maling aan hebben. Het moet dus breed genoeg gedragen en realistisch genoeg zijn om het te kunnen gebruiken om anderen er serieus op aan te spreken. Maar het is precies zoals u zegt: de ontwikkelingen gaan zo snel dat dat alleen al de noodzaak geeft om de druk erop te houden. Dat deel ik zeer. Dat is ook de reden dat wij als Nederland niet hebben gezegd dat we het congres één keer

organiseren en daarna het stokje overdragen, maar dat we daar het voortouw in blijven nemen.

De **voorzitter**:
Ik zie geen verdere interrupties. Ik geef het woord aan de Staatssecretaris.

Staatssecretaris **Tuinman**:
Dank u, voorzitter. Ik ben heel blij dat we in het afgelopen anderhalf jaar ook hier met elkaar in de Kamer wegbewogen zijn van het bespreken van IT en digitalisering als een bedrijfsvoeringsvraagstuk, waarbij het vaak ging over kostenoverschrijdingen en in control zijn, naar een gesprek over digitalisering waarin dat meer is dan bedrijfsvoering. Sterker nog, de digitale impuls kan op dit moment het verschil zijn tussen vrede en conflict. Dat betekent dat we onze digitale slagkracht moeten versterken. Daar staan we zeker niet alleen in. Daarom ben ik vanaf dag één als Staatssecretaris met de Minister aan de slag om de digitalisering van de krijgsmacht in de top drie van prioriteiten te zetten. We hebben die intern, in ons eigen departement, mainstream gemaakt.
Wie de informatiestromen en digitale systemen goed onder controle heeft, beslist sneller, reageert adequater en heeft een beter beeld van wat er aan de hand is. Dan kun je ook het initiatief overnemen of behouden. Ik denk dat je al met 2–0 of 3–0 achterstaat als de digitale slagkracht, de layer die alles met elkaar verbindt, niet goed op orde is, ongeacht hoeveel materieel en mensen je op het slagveld kunt zetten of hoeveel afschrikking je daarmee kunt realiseren. De doelstelling, het motto of de lijfspreuk van onze krijgsmacht is natuurlijk: hoe zorgen we ervoor dat we onze mensen met de juiste middelen en de juiste IT een voordeel geven op het gevechtsveld, zodat ze de kans hebben om dat succes ook uit te buiten? We zien bijvoorbeeld in Oekraïne dat artificial intelligence of edge computing, dat eigenlijk betekent dat je rekenkracht zo ver mogelijk richting de bron naar voren brengt, maar ook dat je ultrasnelle connectiviteit moet hebben, nu al deels de uitkomst van de confrontatie bepaalt. Daarom wil ik nogmaals onderstrepen dat die digitale weerbaarheid en slagkracht geen bijkomstigheid, bedrijfsvoering of side event zijn, maar een noodzakelijke asset en randvoorwaardelijk, zowel voor onze inzetbaarheid en effectiviteit als voor onze afschrikking.
Ik ben blij dat we onze IT-portfoliostrategie uiteindelijk hebben kunnen uitrollen. Die maakt het in een aantal speerpunten concreet en creëert voornamelijk samenhang en wendbaarheid tussen al die verschillende programma's die we hebben. Je ziet namelijk dat de zaken in de digitale ecosystemen ontzettend snel gaan. Een drone of software is leuk, maar drie weken later is die eigenlijk al verouderd en moet je 'm updaten. Dat betekent dat wij daarin als Defensie harde en gerichte keuzes moeten maken. We maken keuzes over hoe we ervoor zorgen dat we de tools in IT en digitalisering zo snel mogelijk uitrollen richting onze mensen, onze warfighters, zodat ze uiteindelijk sneller kunnen leren. Het gaat af en toe ook weleens mis, want er zijn ook projecten waar we geld en effort in steken en waar we uiteindelijk over zeggen: oké, prima, dit heeft niet gewerkt; jammer, maar we moeten door.
Ik wil ook even stilstaan bij een aantal zaken die we hebben gerealiseerd de afgelopen tijd. Een ding is bijvoorbeeld dat de leverbetrouwbaarheid, het daadwerkelijk leveren van meer IT uit de kranen, meer IT-projecten, van 4% naar 70% is gegaan. Ik ben daar heel trots op, ook op beide heren, zowel links als rechts van mij. Met andere woorden, ongeveer een derde tot driekwart van de projecten blijft binnen de tijd en het budget en, nog belangrijker, leveren op wat we met elkaar hebben afgesproken. We hebben dat deels gedaan door die grote projecten op te knippen in concrete stukjes, en ze daar harder op in te voeren.
Een ander mooi voorbeeld is, denk ik, project Foxtrot. Dat gaat over radio's en een modulair versleutelsysteem waarbij we onze militairen

onder de zwaarste omstandigheden kunnen laten optreden in het elektromagnetische spectrum. Daar gebeurt heel veel in. Dat spectrum is eigenlijk alles wat je niet kunt zien, maar wat wel impact heeft op je optreden.
Zelf vind ik JIVC een mooie opsteker, ons IT-bedrijf van Defensie. Ongeveer 2.800 specialisten zijn binnen de overheid eigenlijk de enigen die daadwerkelijk onze eigen IT van begin tot eind kunnen bouwen en kunnen monitoren. Als we met andere bedrijven werken of zaken uitzetten, dan kunnen we daardoor goed functioneren. Computable, een respectabel blad, kijkt ernaar. Dit jaar heeft ons JIVC volgens Computable het beste imago onder niet-IT-bedrijven. De organisatie groeit hard. Wat dat betreft komen we van ver. Ik zie het ook binnen onze eigen IT-organisatie. De sfeer is goed, er lopen veel programmeurs met oefeningen mee. Het is een mooie opsteker.
Nogmaals, de Digitale Transformatie Strategie is echt een instrument om onze militairen beter te ondersteunen en een voordeel te geven. Ze helpt ook om de connectie en de samenwerking met de bondgenoten bij elkaar te krijgen. Het idee dat slagkracht alleen staal, vuur en bullets is, is wel wat outdated. De bits en bytes gaan meer en meer het verschil maken. Daarin moeten we uiteindelijk ook flink blijven investeren.
Dan wil ik nog even stilstaan bij wat algemene zaken, ook met betrekking tot de soevereiniteit. De Minister heeft daar al wat over gezegd. Palantir blijft interessant. De vraag was wie dan eigenlijk de eigenaar is van de data, de analyses en het gebruik ervan. Mevrouw Belhirch vroeg hiernaar, maar ik kan me goed voorstellen dat het ook bij anderen leeft. Nederland, Defensie, blijft altijd eigenaar van de data en ook van de analyses die eruit voortkomen. Die data staan op onze eigen infrastructuur en ook op onze eigen servers. Dat geldt voor wat we doen met Palantir, maar zeker ook voor alle andere software. Laat me daar nog wat meer over uitleggen. Op dit moment hebben wij het twin datacenter. Dat is een eigen datacenter. Het zijn twee verschillende, zodat je daarin wat robuustheid hebt. We zijn eigenaar van alle infrastructuur en de hardware. Als je in contact wilt komen met bijvoorbeeld de software, het platform zelf of de data, dan moet je door dezelfde screening als al onze medewerkers. Wat dat betreft hebben we het goed gelaagd opgebouwd. Onze data zijn van ons en blijven van ons en dat geldt ook voor de applicaties.
Is die software dan niet een soort vendor lock-in, iets waar je nooit meer vanaf komt als je het eenmaal hebt? Dat is niet zo. Palantir is een open standaard. Dat betekent dat wij mee kunnen kijken in de software. Het betekent ook dat als de leverancier of de Verenigde Staten om wat voor reden dan ook zouden zeggen «jullie krijgen geen updates meer», wij altijd de mogelijkheid hebben om met onze eigen IT-infrastructuur, onze eigen platformen en data die applicaties, die software te blijven gebruiken. Het is immers een open standaard.
De heer Erkens vroeg hoe we borgen dat we in de technologische voorhoede van Europa blijven. Dat is min of meer een kerntaak voor deze kant van de tafel of voor het hele departement. Je moet niet de aller-, aller-, allerbeste technologieoplossingen hebben, maar je moet ervoor zorgen dat je technologie hebt die 10% tot 15% beter is dan die van je tegenstanders. Wij moeten er dus voor zorgen dat onze mensen, onze warfighters, altijd een voordeel hebben. Tijd, plaats en technologie-segment maken daarbij niet uit. Je moet niet alleen langetermijndoelen en roadmaps hebben, maar je moet er ook voor zorgen dat de technologie zo snel mogelijk terechtkomt in de operationele omgeving, in scenario's waarin je die technologie kunt gebruiken, zodat je daarvan leert. Het iteratieve vermogen moet hoog zijn.
Dat is één. Twee. Je doet dat niet alleen als krijgsmacht of met andere krijgsmachten, je doet dat in publiek-private samenwerking, het liefst in Nederland of in Europa. Zo kun je als Defensie ook profiteren van ontwikkelingen. Als je kijkt naar het digitale domein, naar cloudoplos-

singen of iets dergelijks, dan zie je dat daarin in de commerciële of private wereld 1.000 miljard of wel meer per jaar wordt geïnvesteerd. Nederland, Europa en de krijgsmacht moeten reëel zijn, dus uiteindelijk wil je daar wel mee samenwerken, maar je moet wel goede soevereine controles instellen. Ik denk dat wij die goed hebben neergezet met de Defensie Strategie voor Industrie en Innovatie en ook de roadmaps op technologische gebieden. We hebben er ook een budget van 1,2 miljard voor vrijgemaakt. Dat is belangrijk om ervoor te zorgen dat we in de voorhoede blijven zitten. Dat geldt voor de echte nichecapaciteit zoals autonomiteit, slimme materialen en space, maar ook voor een aantal basisgebieden.
Een ander voorbeeld is dat we er uiteindelijk in onze strategie voor hebben gekozen om verschillende investeringsvehikels daarin te ondersteunen. Nu is dat helemaal rond. TTT is thematische technologieontwikkeling met Invest-NL. We hebben er ook voor gekozen om met de NWO, de Nederlandse Organisatie voor Wetenschappelijk Onderzoek, 35 miljoen beschikbaar te stellen voor fundamenteel onderzoek dat daarbij past. We hebben nu natuurlijk het SecFund, het Security Fund, met 100 miljoen om die «early»-bedrijven en de start-ups, die voornamelijk bij onze universiteiten vandaan komen, een gezwinde start te geven in die dual-usemarkt. Ik ben het daar dus volledig mee eens. Ik durf zelf ook nog wel te stellen dat we ons als overheid, maar zeker ook als krijgsmacht, gerealiseerd hebben dat het niet alleen gaat om te kijken naar welke capabilities je nodig hebt. Je moet uiteindelijk de industrie, de R&D, daarmee helpen en zo af en toe, zo hier en daar, ook specifiek richten. Zo zorg je ervoor dat onze mensen op elk moment de laatste technologie hebben en daarmee een voordeel hebben ten opzichte van anderen.
Er was een specifieke vraag over kwantum computing en de kwantumcomputer. Dat gaat ook over encryptie. Het gaat eigenlijk over de problematiek van post-kwantumcrypto. Dat is dus dat je met een kwantumcomputer met heel veel rekenkracht alle wachtwoorden kunt breken. Ik wil daarover zeggen dat kwantum in een van de Nederlandse prioriteitsgebieden zit. We hebben er vijf. We hebben ook een roadmap. Die kunt u vinden in de Defensiestrategie. Daar hangt industrie en innovatie onder. Er is een roadmap op het gebied van kwantum. Daar investeren we dus sterk in. Ik ben net terug van een werkbezoek aan Zuid-Korea. Daar zijn ze ook sterk in kwantum. Zij richten zich wat meer op radars. Wij doen wat andere zaken. Ook Zuid-Korea kijkt naar Nederland, omdat we niet alleen op het gebied van onderzoek en R&D, maar ook op het gebied van de krijgsmacht in Nederland een heel sterk ecosysteem hebben.
Het laatste wat ik u toch nog even wil zeggen, is het volgende. We hebben u zes maanden geleden, denk ik, een aantal brieven gestuurd. Die gingen over cryptografie. Hoe zorg je ervoor dat je in Nederland informatie beveiligd kunt uitwisselen? Daar zijn een aantal speciale bedrijven voor. Het gaat uiteindelijk ook over die post-cryptowereld. We hebben een aantal deals met bedrijven gesloten. Enerzijds gaan we strategische partnerschappen aan, zodat het echt in soevereine Nederlandse handen blijft. Anderzijds hebben we er ook zeggenschap in. Dat hebben we in uw Kamer ook vaak besproken. Op verschillende lijnen zijn we daar uiteindelijk mee bezig. Ik moet zeggen dat we daar inderdaad stappen in moeten zetten, zeker weten. Wat mij betreft mag er ook wel wat meer geld naartoe gaan. Maar goed, dat gaan we misschien morgen of overmorgen zien. Het staat echt wel hoog op de agenda. Ik denk dat we er echt de juiste dingen in doen.
Dan was er een aantal vragen over inkoop, aanbesteden en technologie. De heer Van Lanschot had het over inkooptermijnen. Ik kende het voorbeeld niet precies, maar het ging er in elk geval over dat er bij onze eenheden frustratie was over dat er ergens iets niet snel genoeg kon. Ik ben altijd bereid om straks even te bekijken wat dat dan is en of we iets een kickstart kunnen geven. Die inkooptermijnen zijn we sowieso als een

gek aan het terugbrengen. Ik heb u al een aantal keren een brief gestuurd over inkoop en aanbesteden. Het ging eigenlijk over de «voorzieningketen»; zo noemen we dat. Die loopt van de behoefte tot aan de daadwerkelijke realisatie daarvan. Ik kan u zeggen dat we op dit moment 94% van al onze aanbestedingen en inkoop buiten het Europese inkoopkader doen. Dat wil niet zeggen dat we het niet in Europa kopen, maar we doen dat buiten het Europese inkoopkader. Bij hele grote projecten levert ons dat per definitie al 18 tot 22 maanden voordeel op. Dat heet dan «hoofdtaak 1 inkoopkader». Bij eigenlijk alles wat heel concreet te maken heeft met gevechtskracht en afschrikking kunnen we dat op die manier doen. Je kunt dat dan uiteindelijk ook single-source, rechtstreeks, aanbesteden. Dat gaat dus eigenlijk wel goed.
Waar misschien nog een stapje in gezet kan worden, is in onze cultuur. We hebben natuurlijk een hartstikke mooie en superwaardevolle inkoopketen. Daar zitten ook allerlei teams op. Soms is het toch nog wel lastig dat als je twintig jaar je marktverkenningen hebt gedaan, het je professie is, je daarin bent opgeleid en getraind, de Staatssecretaris dan nu tegen je zegt: je krijgt nu 22 maanden voor een marktverkenning, maar neem nu een week de tijd en kom maar met de beste richting. Dus dat is dat, wat dat betreft.

De heer **Van Lanschot** (CDA):
Dank aan de Staatssecretaris voor de mogelijkheid tot het verkennen van deze casus. Dat zullen we buiten de vergadering doen. Ik heb een vraag, namelijk: hoe denkt hij dat wij als Kamer kunnen bijdragen aan de cultuurverandering binnen de inkooporganisatie?

Staatssecretaris **Tuinman**:
Dat is een hele goede vraag, maar misschien krijgt u een antwoord dat u niet wil horen. Op een aantal vlakken is wat onze krijgsmacht nodig heeft rust. Dit is er een van. We hebben in het inkoopproces, de keten en het hele ecosysteem de laatste tijd best wel veel versnelling gebracht. Wat mij betreft is het beleid goed. De methodes die we daarvoor hebben en de inkoopprocessen zijn ook prima. Het heeft nu gewoon even wat rust nodig.
Laat ik nog een aantal andere voorbeelden geven. Ik zat nog in het hoog oververhaal, maar de heer Van Lanschot, en volgens mij ook anderen, verwijzen specifiek naar de vraag hoe je ervoor zorgt dat je sneller inkoopt. Het gaat dan om de behoeftes lager in de organisatie. The boots on the ground are always right, hè. Onze militairen hebben eigenlijk wel gelijk. Hoe zorg je daarvoor? Een voorbeeld is KIXS. Dat is een digitale IT-organisatie die eigenlijk heel dicht tegen de warfighters en capabilities aan IT-oplossingen ontwikkelt, echt gewoon voor op je smartphone. We hebben in de cyberwereld de Cyber Innovation Hub. Daar werken trouwens heel veel reservisten; daar zal ik zo meteen op terugkomen. Dat zorgt er ook voor dat, als onze cybermensen in de praktijk tegen iets aan lopen, je een mechanisme hebt om heel snel iets te ontwikkelen. Daar is ook geld voor. Dan kun je daar ook mee werken.
Het andere punt is dat je meer in die ecosystemen moet denken. In dat kader hebben meneer Van Lanschot en ik het weleens vaker gehad over die publiek-private samenwerking. Dat lukt ook wel. Ik doel op erop dat het voor bedrijven en start-ups met goede ideeën makkelijker gemaakt wordt om eerder toegang te krijgen tot onze militaire eenheden. Een voorbeeld daarvan zijn drones. Je wil dat het gereguleerd is als bijvoorbeeld een 43ste brigade een specifiek dronepeloton aan het ontwikkelen is. Het moet niet één grote vrije speeltuin zijn. Je wil wel dat de bedrijven die in dat ecosysteem zitten, toegang hebben tot die operators en tot die oefeningen, zodat je uiteindelijk die iteraties op het gebied van innovatie veel sneller voor elkaar kunt krijgen.

De heer Erkens vroeg naar zwerfdrones. Dat vind ik trouwens een mooie Nederlandse titel voor swarming. Het zijn ook eigenlijk zwerfdrones. O, «zwerm», hoor ik, niet «zwerf». Zwermdrones. Hij vroeg naar de automatisering daarvan en of we onze eigen bedrijven dan niet onnodig beperken. Ik denk dat juist het tegenovergestelde het geval is. Wij zijn in Nederland van origine niet heel ver op dat gebied. Maar we zijn dat nu als een gek aan het faciliteren. Je ziet wel dat die kennis zit bij onze kennisinstellingen, en ook bij onze universiteiten, maar uiteindelijk moet je dat ook in capabilities en daadwerkelijke producten gaan krijgen.
Ik denk dat het wel goed is om altijd onderscheid te maken tussen verschillende lagen als je het hebt over autonomiteit op het gebied van software. Je hebt het bijvoorbeeld over de autonomiteit met betrekking tot drones zodat ze vliegend kunnen opereren. Je hebt autonomiteit met betrekking tot swarming, dat zwerven, namelijk dat ze met elkaar kunnen communiceren en ergens uit kunnen komen. Je hebt autonomisering op het gebied van communicatie en connectiviteit, namelijk dat het niet uitmaakt of je 5G of iets anders gebruikt. Je hebt ook autonomisering op het gebied van besluitvorming en met betrekking tot doelselectie en dat soort zaken. Je hebt dus allerlei verschillende aspecten in de autonomiteit van systemen. Ik denk dat het goed is dat wij daar specifiek in investeren als Nederland en dat we kijken waar de specifieke ontwikkelbehoeftes zitten en waar we sterk in zijn. Nederland is voornamelijk sterk in het ontwikkelen van specifieke missiemodules.
We hebben er allerlei challenges voor. Een mooi voorbeeld is de counterdrone-challenge. We hebben net vier winnaars daarvan aangewezen. Zeg je «counterdrone» dan denkt iedereen altijd aan een drone met een explosief, maar 90% van wat dat ding uiteindelijk laat werken, is de software en de autonomiteit die die inzet. Je hebt namelijk niet meer de tijd om ervoor te zorgen dat je het juiste doel selecteert, wat de baan moet zijn en dat soort zaken.
Dan ga ik richting het blokje personeel. Laat ik heel duidelijk zijn: we hebben het in deze commissie vaak over materieel, in dit geval over de digitale kant, maar uiteindelijk maakt het menselijk brein het verschil in een gevecht of in de slagkracht. De mensen doen dat. Of het nou gaat over cyber of over onbemande systemen, uiteindelijk zit er altijd ergens een menselijk brein achter dat het moet uitdenken of dat de besluiten moet nemen.
Dan kom ik op de vraag van de heer Van Lanschot – de heer Boon stelde die vraag ook – of we uiteindelijk het personeel, de innovatieve verwervingssystematiek en de maatregelen in het cyberdomein goed bij elkaar kunnen brengen. Dat is zo. Op het gebied van personeel, zeker op het gebied van cyber- en IT-personeel, doen we een paar dingen. Enerzijds moet je dat type mensen meer bij elkaar brengen. De stap die we hebben gezet, is dat we de cyberreservisten uit de algemene poule van reservisten hebben gehaald en ze specifiek bij het DCC hebben ondergebracht. Je krijgt dan community building. Als reservist, als parttimemilitair, ben je niet alleen cyberspecialist. Nee, je moet ook zorgen dat je esprit de corps en dat soort dingen krijgt. Dat is één ding.
Het tweede ding dat we doen, maakt het voor reservisten, zeker voor cyberreservisten, uiteindelijk het meest aantrekkelijk. Dat is niet de salaristabel; daar kom ik zo meteen nog op terug. Het meest aantrekkelijke is dat je aan issues, aan problemen en aan uitdagingen werkt waar je in de private wereld, of ergens anders, niet toe in staat bent.
Ik kreeg ook wat vragen over hoe het personeelsbestand er nu uitziet en over de terugloop. Wij zien op dit moment geen leegloop of verloop. Wij zien het tegenovergestelde. We zien op het gebied van cyberreservisten een ontzettende aantrekkingskracht. Die cijfers gaan eigenlijk juist hartstikke hard omhoog. In Breda hebben bijvoorbeeld 36 mensen de afgelopen initiële reservistenopleiding gehaald, waarvan er 20 cyberreservisten zijn. We zien juist dat het aantrekt.

Een ander voorbeeld is de NAVO-top. We hebben voor de NAVO-top met elkaar een cyber shield gebouwd. Een aantal maanden was Nederland namelijk het toppunt van cyberaanvallen. Het is aardig goed gelukt om dat netwerk dicht te houden. Hoe hebben we dat gedaan? We hebben dat niet alleen met onze veiligheidsdiensten gedaan, zoals DCC en JIVC, die de beveiliging van onze witte systemen doen. We hebben het geïntegreerd met een aantal top-private cybersecuritybedrijven. Het mooie daarvan is dat we daar als overheid en als krijgsmacht samen met de bedrijven zo veel van hebben geleerd dat daar businessmodellen uit voort zijn gekomen die we uiteindelijk weer hebben kunnen vermarkten bij de Europese top in Denemarken. Je ziet dus dat bedrijven in de IT- en cyberwereld eigenlijk ook willen dat hun mensen parttime bij de krijgsmacht aan de slag gaan. We hebben daar op het gebied van reservisten beleid voor. We sluiten eigenlijk heel veel convenanten met bedrijven, want het mag alleen als er in de cao en de arbeidsvoorwaarden een aantal maatregelen genomen worden. We zien juist ook dat bedrijven die in de IT- en de cyberwereld zitten dat uiteindelijk echt goed willen doen. Zij gaan nu met ons aan de slag om die convenanten te sluiten of hebben die daadwerkelijk al gesloten. Dit is dus echt een win-winsituatie. Ik zie dus geen irreguliere uitstroom van IT- en cybermensen.
Ik wil daar nog een paar dingen over zeggen. Als je kijkt naar het IT-personeelsbestand van de krijgsmacht, dan zie je dat het eigenlijk heel goed gaat. Het gaat misschien wel veel beter dan we gedacht hadden. In de afgelopen anderhalf jaar hebben we in ons totale IT-werkbedrijf bijvoorbeeld meer dan 400 nieuwe mensen aangenomen. Dat zijn niet alleen jonge mensen die van de universiteit af komen, maar dat zijn ook mannen en vrouwen die een eigen bedrijf hebben gehad en bij ons aan de slag willen. Zij hebben veel ervaring en zeggen dat ze zich maatschappelijk relevant willen maken in de vijf jaar die ze nog te gaan hebben. Dat is dus wel heel mooi om te zien.
Dan was er nog een vraag over flexibilisering van de salaristabellen. Volgens mij kwam die vraag van de heer Erkens. Ik kan daarover zeggen dat we er wel degelijk naar kijken. Dat doen we ook met een aantal andere specialistencategorieën. Maar dat gaat onderdeel uitmaken van de nieuwe arbeidsvoorwaarden van halverwege 2026, waar we nu de voorbereidingen voor aan het treffen zijn. Ik kan daar niet te veel op vooruitlopen – dat is mogelijk ook iets voor mijn opvolger – maar dat zit daar wel degelijk in. Je moet fatsoenlijk en goed betalen. Dat doen we zeker ook. Maar nogmaals, ik zie over het algemeen dat het zeker voor IT- en cybermensen het allerbelangrijkste is dat ze toegang hebben tot problemen die echt uitdagend zijn. Zolang je dat kunt faciliteren met het DCC, maar ook met een cyberrange waarmee je kunt trainen, gaat dat best wel aardig.
Over de uitstroom van cyberreservisten heb ik het zojuist gehad.
Mevrouw Nanninga had nog een vraag over het tijdsframe van nieuwe mensen binnenhalen op de huidige arbeidsmarkt. Daar ben ik heel simpel in: zo snel mogelijk. We bekijken ook echt wel welke interventies we kunnen doen en hoe we ervoor kunnen zorgen dat we zo attractief mogelijk zijn. We hebben voor cyberreservisten een reservistenacademie opgezet. We hebben ook een cyber innovation and training centre opgericht. We hebben een Cyber Range. Dat is heel interessant. Soms kun je dingen niet in de werkelijke omgeving doen, maar die kun je dan daar in een synthetische digitale omgeving doen. Als je ervoor zorgt dat je mensen uit de praktijk en cyberreservisten samenbrengt en van die deep dives hebt waarbij je moeilijke problemen breekt, vinden zij dat uiteindelijk helemaal geweldig. Dat is hetgeen we nodig hebben.
Volgens mij was het de heer Boon die vroeg: hoe zorg je er nou voor dat je die IT- en die cyberkennis niet alleen bij je specialisten hebt zitten? Het is eigenlijk tweeledig. In een reservistenopleiding zitten sowieso een aantal cyberawarenesszaken. Dat is een. In alle carrièrecursussen die we hebben voor officieren en onderofficieren zit het uiteindelijk altijd. Het is

ook belangrijk dat bijvoorbeeld een DCC geen gesloten systeem is. Je moet mensen kennis en ervaring laten opdoen. Het is ook wel goed als die bijvoorbeeld doorstromen naar een CEMA-eenheid. Dat is een eenheid binnen onze krijgsmacht. Het is goed als je dat uiteindelijk doet. Dat is een aantal manieren waarop we proberen dat voor elkaar te krijgen.
We hebben het ook gehad over de publiek-private samenwerking met betrekking tot bedrijven. De heer Van Duijvenvoorde had een goede vraag over de arbeidsmarkt. Dat is echt wel heel interessant. Ik denk dat we hier op het departement nu een jaar mee bezig zijn. We hebben er ook wat onderzoek naar laten doen. Ik ben ook blij dat bijvoorbeeld het CPB, maar ook SEO, het economische onderzoeksinstituut van Rotterdam, hier uiteindelijk aandacht aan besteedt. We hebben het vaak over een krappe arbeidsmarkt. Dat klopt, maar de arbeidsmarkt is op dit moment aan het verruimen. We zaten rond de 3%, maar we zitten nu op 4,2%. Die arbeidsmarkt is dus wel wat aan het verruimen. Dat is het eerste. Dan het tweede. De echte groei van de krijgsmacht is uiteindelijk reservecapaciteit, dus parttimemilitairen. Parttimemilitair betekent dat de civiele werkgever of een andere overheidsinstantie de dominante werkgever is. De rest doe je bij ons. Gemiddeld werkt een Nederlandse arbeider – laat ik het zo netjes zeggen – 28 tot 32 uur per week. Ik wil niet zeggen dat die die andere 8 uur mooi bij de krijgsmacht kan werken. Nou, eigenlijk wil ik dat wel zeggen. Dan doe je niet alleen een mooie ervaring op, maar bouw je ook een sociaal netwerk. Je kunt er ook bij sporten. Dat is wel een ding. Je ziet dat er in de Nederlandse arbeidsmarkt wel degelijk nog ruimte zit. Er is ook wel ruimte in de arbeidsproductiviteit en in hoe je het uiteindelijk bij elkaar brengt.
Het volgende is ook belangrijk. Ik denk dat we nu met betrekking tot reservisten 400 convenanten hebben getekend met grote en kleine bedrijven in allerlei sectoren. Daarbij maken we afspraken. Ik ga niet zeggen wie het is, maar we hebben een deal getekend met de grootste Nederlandse telecomaanbieder en die zegt: vanuit de werkgever krijg je twintig dagen in het jaar om als reservist aan de slag te gaan. Die ziet aan de andere kant ook dat het belangrijk is dat die kennis en ervaring worden meegebracht. Het is ook heel mooi dat we de Nationale Weerbaarheids-training zijn gestart. Een van de drie sporen is met werkgevers. Een voedingswarenleverancier heeft een aantal collega's de ruimte geboden om die Nationale Weerbaarheidstraining te doen. Eentje heeft het ook gehaald. Het is tien weken op kosten, nou ja, eigenlijk in de tijd van de werkgever. Waarom? Omdat de werkgever zegt: «Als je tien weken die Nationale Weerbaarheidstraining doet, leer je iets over leiderschap en doorzettingsvermogen. Dat past in jouw management- en leiderschaps-journey binnen ons bedrijf, dus dan willen we graag dat je daarbij betrokken bent.»
We zien dus bij al die zaken dat je dat wel degelijk op een slimme manier kunt doen. Ik besef dat er met betrekking tot een aantal specifieke schaarse categorieën wel degelijk druk ontstaat in de arbeidsmarkt. Een voorbeeld daarvan zijn vliegers. We hebben meer vliegers nodig, want op dit moment zijn niet alle functies vol. KLM heeft ook meer vliegers nodig. Dan moet je er dus met elkaar afspraken over maken. Daar moet je eerlijk over zijn. Met KLM hebben we dat ook gedaan door een tijdje terug een convenant af te sluiten. Het punt is: zowel op vliegers als op technisch onderhoudspersoneel is wat je moet doen heel simpel. Je moet voor allebei meer mensen gaan aannemen en meer mensen gaan opleiden. Het tweede dat je moet doen, is goed kijken naar waar het probleem ligt en dat aantrekkelijker maken. Als wij als Defensie al het onderhoud doen in Woensdrecht, wil dat niet zeggen dat je dan de hele potentiële populatie in Nederland … Als jij in Groningen zit, wil je misschien niet altijd in Woensdrecht werken, of omgekeerd, of misschien wil je dat juist wel. Je moet naar levensloopregelingen gaan kijken, en uiteindelijk daar gewoon meer in samenwerken. Dat moet je slim doen. Ik vind het een

heel mooi model. Ik vind het helemaal prima. Als jij in je jonge jaren bij ons begint, ga je direct sleutelen aan een F-35. Dat is echt wel shit-hot. Dat is echt nogal een ding. Je doet mooi tien jaar ervaring op. Dan wil je misschien in Amsterdam of Groningen een huis kopen en je gezin onderhouden. Hartstikke mooi. Dan kun je misschien een aantal jaar bij KLM, Transavia of TUI aan de slag. Als je dan wat ouder bent, kun je zeggen: «De kinderen zijn uit huis. Ik wil nog een paar jaar de nieuwe jongelui wijs maken, opleiden, trainen. Ik wil wat doen aan de maatschappelijke weerbaarheid van Nederland.» Ik zie dat er steeds meer behoefte is aan dit soort trajecten en de levensloopregelingen. Dat zijn we wel aan het inregelen. We zijn er denk ik, net als zij aan de bedrijfskant, nog wat te star in. Maar je moet het met elkaar wel goed gaan regelen. Ik zie daar dus wel degelijk een win-win in zitten.
Dan ben ik, als het goed is, door mijn inbreng heen. Als er geen vragen zijn, zou ik straks nog even een woordje van dank uit willen spreken. Het zou namelijk zomaar mijn laatste debat kunnen zijn.

De **voorzitter**:
Dank u wel. Daar geef ik u aan het einde natuurlijk voldoende tijd voor. Voordat ik naar de tweede termijn ga, wil ik toch namens de commissie ook even terugkomen op de woorden van de Minister over Afghanistan. Het is heel goed dat u dat zelf ook aankaart, want ik denk dat we met z'n allen met veel verbazing hebben gekeken naar de uitspraken van Trump. Het is zeer kwetsend voor de veteranen en hun nabestaanden. De bewoording is ook onjuist. Als Nederland hebben we ruim 30.000 militairen naar Afghanistan gestuurd. Daarvan hebben, als ik het goed heb, 25 mensen daar ook hun leven gegeven. Zelf ben ik twee keer in Afghanistan geweest en heb ik gezien wat onze mannen en vrouwen daar hebben gedaan. Het is belangrijk dat ze de erkenning en waardering krijgen die ze verdienen. Daarom ben ik blij dat de Minister dit heeft aangekaart bij de ambassadeur en dat het inderdaad ook terechtkomt bij Trump en de VS-administratie. Dit moet inderdaad zeer streng veroordeeld worden. Dat hebben andere landen, zoals Italië, en andere collega's ook gedaan. Ik dank de Minister daar dus voor. Dit zou zomaar eens op een ander moment weer terug kunnen komen.
Dan beginnen we met de tweede termijn. Ik begreep dat uw spreektijd 1 minuut en 20 seconden is – dat is ongeveer anderhalve minuut. Ik begin bij de heer Van Lanschot.

De heer **Van Lanschot** (CDA):
Dank, voorzitter. Ik sluit me geheel aan bij uw laatste woorden over de NAVO-missie. Onze fractie vermoedde inderdaad ook al dat dit zomaar het laatste commissiedebat met de Staatssecretaris zou kunnen zijn. Wij zouden hem hier dus ook graag met een woord van dank willen toespreken. Dat is om twee redenen. Dat is niet alleen om zijn onvermoeibare drive, maar ook om het terugbrengen van de esprit de corps. Dat laatste noemde hij net zelf al. Defensie heeft het de afgelopen jaren natuurlijk zwaar gehad. Dan is het fijn als er iemand is die zelf ook uit de militaire organisatie komt om die esprit de corps terug te brengen. Veel dank daarvoor. Ook tijdens dit debat hebben we weer kunnen zien hoe breed de interesse van de Staatssecretaris is, van Defensity College tot post-kwantum en – wat hebben we nog meer langs gekregen? – drones. Het enthousiasme van de Staatssecretaris is grenzeloos. Veel dank daarvoor. Ten tweede merk ik op dat de Staatssecretaris een zeer inspirerend voorbeeld is van een carrièrepad dat zowel Defensie als de politiek met zich meebrengt. Ik hoop dat we dat vaker gaan zien de komende jaren. Veel dank dus.

De **voorzitter**:
Dank u wel. Dan de heer Erkens.

De heer **Erkens** (VVD):
Voorzitter. Van mij geen inbreng voor de tweede termijn, maar inderdaad ook een woord van dank aan de Staatssecretaris. Wij zijn in de vorige periode met elkaar opgegroeid toen we samen als woordvoerders Defensie in deze commissie zaten. Ik denk dat ik wel kan zeggen, ook namens de VVD-fractie, dat de heer Tuinman op een aantal dossiers echt de bakens heeft verzet sinds hij Staatssecretaris is. Hij heeft er een drive in gebracht, en ook een bepaald ongeduld om processen waar we misschien normaal vijf, zes, zeven jaar over doen, er in vijf, zes, zeven weken door te krijgen. Dat is precies de mindset die we ook de komende jaren nodig zullen blijven hebben om Nederland veilig te houden en Defensie op te bouwen op de vlakken waar het de laatste decennia, natuurlijk ook door een gebrek aan geld, verzwakt is geraakt. Alle complimenten dus ook van mij. En als Staatssecretaris Tuinman eraan hecht, kunnen we ze ook gewoon «zwerfdrones» noemen in plaats van «zwermdrones».

De **voorzitter**:
Dank u wel. De heer Boon.

De heer **Boon** (PVV):
Voorzitter. Ook ik wil de Minister bedanken voor zijn woorden. Ik ben zelf ook in Afghanistan geweest en ik heb samen met de militairen vooraan gevochten. Ik ben dus een van die militairen. Het doet mij goed dat de Minister er zo op zit. Ook de Staatssecretaris wil ik bedanken voor zijn werkzaamheden, en dan niet alleen voor de werkzaamheden hier maar ook voor zijn militaire werkzaamheden, waardoor hij altijd een held blijft voor velen.

De **voorzitter**:
Mooie woorden. Mevrouw Nanninga.

Mevrouw **Nanninga** (JA21):
Dank, voorzitter. De JA21-fractie heeft veel waardering voor en instemming met de goede woorden van de Minister over de eer die onze Afghanistanveteranen en hun nabestaanden toekomt. Dat is zeer belangrijk; daar ben ik het mee eens. Ook natuurlijk een woord van dank voor de hele korte maar ook hele prettige samenwerking die wij mochten hebben met de Staatssecretaris. Het gaat hem goed. Daar ben ik van overtuigd, want dit was geen wens maar een constatering! We hebben hem immers een beetje leren kennen. Zoals de sprekers voor mij ook al zeiden, is het heel goed om dat elan en die praktijkervaring in deze rol te hebben. Die heeft de Staatssecretaris naar het oordeel van JA21 ook ten volle benut. Heel veel dank daarvoor dus.

De **voorzitter**:
De heer Van Duijvenvoorde.

De heer **Van Duijvenvoorde** (FVD):
De dichter Willem Jan Otten heeft een van de mooiste zinnen geschreven over het moment waarop hij een vrouw ontmoet. Nu is dat niet onze band, maar hij schrijft daarover: ik wist al dat ik je zou gaan missen op het eerste gezicht. Dit is mijn eerste debat met de Staatssecretaris en ik vind het jammer dat we niet meer debatten hebben kunnen doen. Ik vond de antwoorden erg inspirerend. Het is natuurlijk heel bijzonder, zoals Maes ook zei, dat iemand uit het veld hier meehelpt, meedenkt en meedoet met het beleid. Het is jammer dat we niet meer debatten gaan hebben. Wat de Minister zei over Afghanistan ondersteun ik natuurlijk ook helemaal, namelijk dat daar heel veel gebeurd is en dat dat wel erkend moet worden, en dat we dat ook zullen blijven doen. Dank jullie wel.

De **voorzitter**:
Dank u wel. Dan geef ik het voorzitterschap even aan de heer Erkens.

Voorzitter: Erkens

De **voorzitter**:
Dan geef ik het woord direct aan u.

Mevrouw **Belhirch** (D66):
Het hoefde eigenlijk niet, want ik wilde ook iets zeggen als voorzitter. Er is al veel gezegd over de Staatssecretaris, dus wat valt er eigenlijk nog te zeggen behalve dat we als commissie en ook persoonlijk veel hebben genoten van uw inbreng, waarin niet alleen de passie opviel, maar ook de inzichten en de vele voorbeelden. Het waren soms minicolleges, maar met veel humor. Ik denk dat dat misschien ook een van de redenen is waarom er meer mensen naar Defensie willen. Het enthousiasme spat er namelijk van af, maar ook de ernst en de energie. Ik wil u heel graag bedanken voor uw inzet en voor de fijne samenwerking en ik wens u heel veel goeds. Dank u wel.

Voorzitter: Belhirch

De **voorzitter**:
En daarmee sluit ik deze vergadering. O nee, u wilde nog wat zeggen! Excuses. Het woord is aan de Staatssecretaris.

Staatssecretaris **Tuinman**:
Dank u wel. Ook een dankwoord vanuit mij. Het nieuwe coalitieakkoord is er, of is aanstaande, dus wat dat betreft zal dit wel mijn laatste debat zijn, met een lach en een traan. Anderhalf jaar geleden ben ik vanuit jullie gelederen gevraagd om de rol van Staatssecretaris op mij te nemen. Volgens mij waren mijn eerste woorden toen: ik ben geen Staatssecretaris van Defensie maar een Staatssecretaris van leveren, leveren en leveren. Dat houdt nu, na anderhalf jaar, op, maar ik denk dat we, samen met de Minister, met Ruben, en het hele team dat hier zit, gezorgd hebben voor een historisch nauwe samenwerking tussen de Kamer en de krijgsmacht. We zijn namelijk allemaal doordrongen van de ernst en van wat er allemaal moet gebeuren. Alle respect en dank dus daarvoor.
Wat betreft personeel denk ik dat we echt te maken hebben met een trendbreuk, en dat we daarbij het doel van meer dan 80.000 medewerkers gaan halen.
Op het gebied van space en technologie hebben we ook een grote stap gezet, denk ik. We gaan eigen satellieten bouwen en de lucht in lanceren: kleine en grote satellieten, met innovatieve materieelkeuzes. We werken aan onze strategische autonomie met eyes in the sky. Op het gebied van materieel doen we dat met modernisering en meer spullen. Het industriebeleid is daarbij misschien nog een tip voor de partijen die straks de volgende stappen gaan zetten. Daar mag wat mij betreft nog wel een vervolg op komen.
Ik ben begonnen met de digitalisering. Ik ben blij dat dit weg is bij bedrijfsvoering en onderdeel wordt van gevechtskracht. Gevechtskracht is personele gereedheid plus materiële gereedheid plus digitale gereedheid. Door dat allemaal in een operationele omgeving, op basis van scenario's en training, te brengen – dat weet de heer Boon – ontstaat uiteindelijk pas gevechtskracht. Daar ben ik dus blij mee.
Ik denk soms nog terug aan alle gesprekken die ik heb gevoerd door heel Nederland over het Nationaal Programma Ruimte voor Defensie. Dit moet gebeuren, dus ik ben blij dat we nu in de volgende fase van de uitvoering zitten. Ik vind wel dat we ons allemaal moeten realiseren dat dit ook pijn doet. Overal in Nederland betalen mensen de prijs voor onze veiligheid.

Dat betekent dat sommigen hun bedrijf moeten stoppen, een bedrijf dat ze soms met hun eigen handen en die van hun voorgangers in de afgelopen 200 jaar hebben opgebouwd. Dat is nu niet meer hun plek. Dat is een offer dat niet alleen door onze militairen wordt gebracht – daar hebben we het over gehad – maar door ons als samenleving. Daar hebben we allemaal belang bij.
Op mijn Kamerlidmaatschap heb ik altijd mooi teruggekeken. Ik voelde me eigenlijk altijd als een vis in het water. In Nederland zijn we wat chaotisch, maar het werkt wel. Daar wil ik u voor danken. Ik wil VVD, D66 en CDA succes wensen met de volgende stap. Jullie succes is ook een beetje ons succes.
Dank u wel.

De **voorzitter**:
Dank u wel. Ik zie dat de Minister geen verdere opmerkingen heeft. Dan sluit ik af. Dank u wel en nog een fijne dag.

Sluiting 12.24 uur.