Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

438

Vragen van de leden **Olger van Dijk** en **Six-Dijkstra** (beiden Nieuw Sociaal Contract) aan de Ministers van Defensie, van Justitie en Veiligheid en van Infrastructuur en Waterstaat over *het bericht «Minister van Defensie: Nederlandse wetten ongeschikt voor «grijze zone» tussen oorlog en vrede»* (ingezonden 8 oktober 2024).

Antwoord van Minister **Brekelmans** (Defensie), van Minister **Van Weel** (Justitie en Veiligheid), van Minister **Madlener** (Infrastructuur en Waterstaat) en van Staatssecretaris **Tuinman** (Defensie) (ontvangen 4 november 2024).

Vraag 1
Heeft u kennisgenomen van het bericht d.d. 3 oktober 2024, getiteld «Minister van Defensie: Nederlandse wetten ongeschikt voor «grijze zone» tussen oorlog en vrede»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u toelichten waaruit het huidige handelingsrepertoire van Defensie bestaat met betrekking tot de Russische schepen die vermoedelijk de Noordzee infrastructuur in kaart brengen om deze later mogelijk onklaar te kunnen maken? Wordt er nagedacht over de uitbreiding van het huidige handelingsrepertoire in de huidige «grijze zone» tussen oorlog en vrede? En zo ja, is de huidige capaciteit op de Noordzee toereikend ten aanzien van deze uitbreiding?

Antwoord 2
Het kabinet beschikt over verschillende manieren om op mogelijke dreigingen te reageren, waar het handelingsrepertoire van Defensie deel van uitmaakt. Het kabinet doet publiekelijk op voorhand geen uitspraken over hoe de Nederlandse overheid handelt bij specifieke voorvallen, om te voorkomen dat kwaadwillende partijen in hun handelen kunnen anticiperen op Nederlandse handelwijzen.

[1] Het Financieele Dagblad, 3 oktober 2024, Minister van Defensie: Nederlandse wetten ongeschikt voor «grijze zone» tussen oorlog en vrede». https://fd.nl/politiek/1532666/minister-van-defensie-nederlandse-wetten-ongeschikt-voor-grijze-zone-tussen-oorlog-en-vrede

ah-tk-20242025-438
ISSN 0921 - 7398
's-Gravenhage 2024

Defensie draagt op verschillende manieren bij aan de bescherming van de vitale infrastructuur op de Noordzee, binnen de kaders van wat Defensie in vredestijd mag. De MIVD voert onderzoeken uit naar heimelijke activiteiten van statelijke actoren die een mogelijk risico stellen voor de nationale veiligheid, zo ook op de Noordzee. Verder heeft Defensie sinds juli 2023 een permanente taak op de Noordzee. In het kader van deze taak doet Defensie aan beeldopbouw en houdt daarmee zicht op mogelijke dreigingen. Daartoe heeft Defensie diverse maatregelen in uitvoering om vroegtijdig heimelijke activiteiten te detecteren, identificeren en attribueren. Zo investeert Defensie in additionele waarnemingscapaciteit op zee en verwerft Defensie vaartuigen met kleine bemanning en onderwatercapaciteiten, die kunnen worden ingezet om dreigingen op zee op te sporen en nader te onderzoeken. Ook escorteert de marine wanneer nodig verdachte schepen en ontmoedigt daarmee de mogelijke ontplooiing van kwaadwillende activiteiten. Tot slot kan de krijgsmacht, in lijn met de derde hoofdtaak, militaire bijstand leveren aan bevoegd civiel gezag om onze infrastructuur veilig te houden.
Verder vraagt de bescherming van vitale infrastructuur van de Noordzee ook om preventieve maatregelen, zoals het verhogen van de weerbaarheid van dit type infrastructuur. Vanuit het interdepartementale Programma Bescherming Noordzee Infrastructuur worden onder andere extra maatregelen genomen om de weerbaarheid van de vitale infrastructuur op de Noordzee te verhogen. Daarom heeft het vorige kabinet besloten om te investeren in het interdepartementale Actieplan strategie ter bescherming Noordzee infrastructuur voor de jaren 2024 en 2025. Ook het huidige kabinet is voornemens om extra te investeren in de bescherming van de Noordzee infrastructuur. Door middel van het Actieplan wordt ook de detectie en duiding van dreigingen op de Noordzee verbeterd, wat leidt tot een snellere reactie als zich verdachte situaties voordoen. Op korte termijn worden belangrijke stappen gezet, waaronder het inkopen van satellietbeelden en de inhuur van patrouillecapaciteit. Daarnaast wordt er onderzoek gedaan naar de meest kwetsbare infrastructuurpunten en het uitrollen van additionele sensoren op de Noordzee. Ook wordt er geïnvesteerd in de ontwikkeling van nieuwe technologieën, zoals bijvoorbeeld met de oprichting van het Seabed Security Experimentation Centre (SeaSEC). Tot slot wordt er gewerkt aan de realisatie van een Alliantie tussen publieke en private partijen om informatie-uitwisseling te versterken voor een verbeterde bescherming van de infrastructuur op de Noordzee. Over dit Actieplan en de investeringen in de jaren 2024 en 2025 is uw Kamer afgelopen voorjaar per brief geïnformeerd. Eind dit jaar wordt de Kamer geïnformeerd over de voortgang hiervan.

Vraag 3
Is reeds in kaart gebracht welke wegen, bruggen en sporen versterkt dienen te worden voor zware militaire transporten? Zo ja, is de Tweede Kamer daar, al dan niet vertrouwelijk, over te informeren? Wordt dit samen ontwikkeld door de betrokken bewindspersonen en zijn hier financiële middelen voor beschikbaar?

Antwoord 3
De Ministeries van IenW en Defensie werken intensief samen aan de verbetering en instandhouding van het wegen- en spoorwegennet in Nederland ten behoeve van militaire transporten.
In 2019 is in opdracht van IenW een uitgebreide analyse van het transportnetwerk van Nederland gemaakt, op basis van de destijds geldende militaire eisen voor militaire mobiliteit en gedefinieerde routes. De Kamer is over de uitkomsten hiervan geïnformeerd (Kamerstuk 21 501, nr. 33). In 2023 heeft de Europese Unie deze eisen en routes geëvalueerd en aangepast. Het transportnetwerk voor militaire mobiliteit wordt daarom opnieuw geëvalueerd door Defensie en IenW, in samenwerking met relevante partijen als Rijkswaterstaat (RWS) en ProRail. Aan de hand van deze evaluatie worden op dit moment knelpunten geïnventariseerd. Op basis van de inventarisatie zal bekeken worden welke knelpunten prioriteit hebben en in de meerjarenprogrammering van RWS kunnen worden opgenomen. Specifieke informatie over militaire transportroutes en corridors kan i.v.m. het vertrouwelijke karakter van deze informatie niet publiekelijk gedeeld worden. Wel heeft Defensie uw Kamer eerder geïnformeerd over het Nationaal Plan Militaire Mobiliteit (Kamerstuk 35 570 X, nr. 75). De implementatie van dit plan richt zich onder

andere op de inrichting van drie multimodale corridors, met routes de geschikt moeten zijn voor grootschalige verplaatsingen van militair materieel vanuit de verbonden zeehavens naar het Europese achterland.
Bij de verbetering van en instandhouding van de transportinfrastructuur voor militaire mobiliteit, wordt ook bekeken welke financieringsmogelijkheden er zijn. Voor het treffen van infrastructurele maatregelen ten behoeve van zwaar militair transport zijn op dit moment geen specifieke (aparte) financiële middelen bij IenW en Defensie beschikbaar. De Europese Commissie beschikt over financieringsprogramma's voor cofinanciering van zogenaamde dual use infrastructurele projecten, die zowel civiele als militaire mobiliteit verbeteren. Voorbeelden van eerdere projecten die met Europese cofinanciering zijn gerealiseerd zijn de uitbreiding van een spooraansluiting in de haven van Vlissingen en de aanpassing van een vijftal spooremplacementen voor treinen met een lengte van 740 meter. Momenteel wordt door het Directorate-General for Mobility and Transport (DG MOVE) gewerkt aan de voorbereiding van een nieuw co-financieringsfonds voor het aankomende meerjarig financieel kader. IenW en Defensie hebben in dit kader gezamenlijk voorstellen gedaan voor mogelijke projecten op de belangrijkste voor militaire mobiliteit gebruikte transportroutes.

Vraag 4
Wat is uw visie op het advies van RAND dat een vorm van (actieve) dienstplicht de betrokkenheid van Nederlandse burgers, en daarmee de weerbaarheid van de samenleving, zou kunnen vergroten? Zou volgens u een vorm van dienstplicht naar Scandinavisch model met een gradueel verplichtend karakter bovendien een wenselijke toevoeging kunnen zijn aan het opschalen van het Dienjaar en het werven van meer reservisten in het licht van de personele uitdagingen bij Defensie?

Antwoord 4
In de Defensienota 2024: Sterk, slim en samen (Kamerstuk 36 295, nr. 1) heeft Defensie plannen gepresenteerd om de juiste en voldoende mensen te vinden, te binden, te behouden en het beste in hen naar boven te halen. Dat is nu de grootste uitdaging waar Defensie voor staat. Defensie werkt in hoog tempo toe naar een schaalbare krijgsmacht en voert een dienmodel in dat daarbij past. Deze schaalbare krijgsmacht krijgt vorm in een organisatie die is ingericht op taakuitvoering door vaste en mobilisabele organisatiedelen. Hierin werken militairen in actieve dienst, burgerpersoneel, reservisten en dienjaarmilitairen in wisselende samenstellingen. Zoals aangekondigd door mijn ambtsvoorganger in de brief van 3 juni jl. (Kamerstuk 36 124, nr. 45), verkent Defensie de mogelijkheden voor een dienmodel dat ook voorziet in maatregelen met een (gradueel) meer verplichtend karakter tussen vredestijd en oorlogstijd. Want er zijn effectievere manieren om op te schalen en de personele gereedheid te verhogen dan een generieke opkomstplicht. Als eerste stap zal een vrijwillige enquête worden ingevoerd. Deze enquête wordt een instrument dat beoogt het dienmodel en daarmee de schaalbare krijgsmacht als geheel te ondersteunen. De enquête richt zich op een bredere doelgroep van jongeren, in de leeftijd van 18–27 jaar. Ook breidt Defensie het aantal reservisten uit en gaat Defensie voortaan minder vrijblijvend om met reservisten, door ze in te bedden in de organisatie. Het aantal dienjaarmilitairen wordt uitgebreid om structureel te beschikken over meer militairen. Defensie richt zich daarnaast nadrukkelijk op specifieke doelgroepen; zo wordt meer aandacht besteed aan het werven van vrouwen – en andere groepen die nu onbedoeld onvoldoende worden bereikt.

Vraag 5
Wat is uw reactie op de suggestie van RAND dat «Den Haag lessen kan trekken van Estland, dat één vast aanspreekpunt heeft aangesteld voor bedrijven in het geval van cyberdreigingen»?

Antwoord 5
In de Nederlandse Cybersecuritystrategie (NLCS 2022–2028) zijn de ambities en acties voor een digitaal weerbare samenleving opgenomen. Met de NLCS worden door het kabinet verschillende acties ondernomen om ongewenste versnippering binnen het cybersecuritystelsel tegen te gaan. Zo worden het NCSC, Digital Trust Centre (DTC) en het Computer Security Incident Response

Team voor digitale diensten (CSIRT-DSP) vanaf 2026 tot één centraal expertisecentrum en informatieknooppunt samengevoegd. Deze nationale cybersecurity organisatie zal organisaties in Nederland, groot of klein, publiek of privaat, vitaal- of niet-vitaal, onder meer van relevante informatie en kennis over dreigingen en incidenten voorzien en waar mogelijk ook verdere hulp bieden bij incidenten.
Daarnaast is er echter ook behoefte aan decentrale cybersecurity expertise. Om er bijvoorbeeld voor te zorgen dat organisaties goed weten om te gaan met dreigingen is het van belang dat daar goede informatie over beschikbaar is. Met de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) naar het Cyberweerbaarheidsnetwerk (CWN) zorgt het kabinet ervoor dat algemene informatie over digitale veiligheid en specifieke dreigings- en risico-informatie zo veel als mogelijk breed zal worden gedeeld, met als doel de weerbaarheid en slagkracht van hun achterbannen van schakelorganisaties te verhogen. Op deze manier combineren we sectorspecifieke kennis met cybersecurity expertise. In de visie op het CWN is de behoefte geadresseerd dat er meer regie nodig is op het netwerk als geheel en op de uitvoering daarvan. Het Nationaal Cybersecurity Centrum (NCSC) treedt op als uitvoeringscoördinator binnen het netwerk. Het CWN staat onder beleidsmatige verantwoordelijkheid van de NCTV.

Vraag 6
Waar ziet het kabinet nog de grootste kansen voor Nederland wat betreft het bevorderen van de nationale digitale weerbaarheid in tijden van oorlogsdreiging?

Antwoord 6
Cyberactiviteiten lenen zich bij uitstek voor hybride conflictvoering onder de grens van gewapend conflict. Nederland bevindt zich reeds in de grijze zone tussen vrede en conflict, waar we toenemende hybride aanvallen zien, zoals in het cyberdomein.
In de NLCS zijn de ambities en acties voor een digitaal weerbare samenleving opgenomen[2]. Met deze maatschappij brede aanpak zet het kabinet in op het verhogen van de digitale weerbaarheid van Nederland door o.a. het intensiveren van de samenwerking op het gebied van informatiedeling en analyse van cyberdreigingen en -incidenten tussen publieke- en private organisaties in het kader van het programma Cyclotron van het Cyberweerbaarheidsnetwerk. Daarnaast wordt er ook gewerkt aan de randvoorwaarden zoals voldoende gekwalificeerd personeel en bewustzijn bij burgers. Uw Kamer wordt spoedig geïnformeerd over de voortgang van deze strategie. Daarnaast ontvangt uw Kamer voor het einde van het jaar een Kamerbrief over de maatschappijbrede aanpak voor de weerbaarheid tegen militaire en hybride dreigingen. De NLCS draagt voor het digitale domein in grote mate bij aan de weerbaarheid tegen dit type dreigingen.
Verdergaande samenwerking tussen overheidsorganisaties om te komen tot een zo actueel mogelijk situationeel beeld is van groot belang, voor het nemen van preventieve maatregelen en het organiseren van adequate incident respons tot aan het actief verstoren, opsporen en vervolgen. Dit geldt te meer in tijden van toegenomen oorlogsdreiging. Ten behoeve van het verhogen van de digitale weerbaarheid van publieke en private organisaties in Nederland is daarnaast de totstandbrenging van wetgeving, zoals de Cyberbeveiligingswet, een belangrijke stap om de digitale weerbaarheid van Nederland te verhogen.[3] Daarnaast zet de overheid in op intensieve publiek-private informatie uitwisseling die aansluit bij de behoefte van de doelgroepen, dit doet het kabinet onder meer door de bovengenoemde doorontwikkeling van het Cyberweerbaarheidsnetwerk en het programma Cyclotron.

---

[2] Actieplan Nederlandse Cybersecuritystrategie 2022–2028. https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022---2023

[3] Met de Cyberbeveiligingswet, waarmee de Europese NIS2 richtlijn wordt geïmplementeerd én die naar verwachting in het najaar van 2025 in werking treedt, worden ongeveer 8000 organisaties in Nederland verplicht tot het nemen van passende en evenredige maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. Dit zal de digitale weerbaarheid van Nederland verhogen.

Het kabinet ziet kansen in het vergroten van de slagkracht van de cybercapaciteiten van Defensie in dit grijze gebied. Met de nieuwe Defensie Cyberstrategie (publicatie voorzien in Q1 2025) die past binnen de kapstok van de NLCSgeeft Defensie richting aan hoe haar cybercapaciteiten doeltreffender in te zetten. We blijven investeren in de cybercapaciteiten van de MIVD en de krijgsmacht. Met de «Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensieve cyberprogramma» kunnen de diensten hun capaciteiten sneller en beter benutten.
Daarnaast is het van belang dat de hele krijgsmacht in het hier en nu effectief en op basis van passende juridische kaders kan oefenen en optreden. Hierbij horen bevoegdheden afhankelijk van de taakstelling en de gereedstellingsstatus van de krijgsmacht. Defensie werkt hiertoe aan passende wet- en regelgeving. Aspecten voor effectief optreden in het cyberdomein in het grijze gebied worden hierin meegenomen.

Vraag 7
Erkent u dat het Nederlandse cybersecuritystelsel bovengemiddeld complex en gesegmenteerd is ten opzichte van andere EU-landen als Duitsland, Frankrijk en België, waar met respectievelijk BSI, ANSSI en CCB één aangewezen cyberautoriteit bestaat verantwoordelijk voor beleid en uitvoering? Hoe kijkt het kabinet aan tegen de benadering van andere EU-landen? Welke lessen kan Nederland daaruit trekken?

Antwoord 7
In het antwoord op vraag 5 is reeds benoemd dat er met de NLCS verschillende acties worden ondernomen om ongewenste versnippering binnen het cybersecuritystelsel tegen te gaan.
De voorbeelden die genoemd worden, Duitsland, Frankrijk en België hebben een andere constitutionele basis. De centrale belegging van bijvoorbeeld de Franse Cybersecurity Autoriteit (ANSSI) is mogelijk in Frankrijk dankzij de executieve macht die bij de Franse President ligt. In Nederland heeft elk ministerie een eigen verantwoordelijkheid en is er veelal gekozen voor een scheiding tussen de taken van uitvoering en beleid.