Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

28 676 NAVO

Nr. 274 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juni 2017

Inleiding

Hierbij bied ik u de geannoteerde agenda aan ten behoeve van de bijeenkomst van de Navo-ministers van Defensie op 29 juni a.s. te Brussel. De bijeenkomst begint met een vergadering van de *Nuclear Planning Group*. Tijdens de werklunch en de werksessie spreken de ministers over de jaarlijkse rapportages over de lastenverdeling, de training van de *follow-on forces*, de EU-Navo samenwerking, de aanpassing van de Navo-commandostructuur en terrorismebestrijding. Na de werksessie is er een bijeenkomst van de landen die bijdragen leveren aan de *Resolute Support* missie in Afghanistan.

In de bijlage bij deze brief ga ik in op mijn toezegging, tijdens het algemeen overleg op 23 mei jl. (Kamerstuk 28 676, nr. 272), om een toelichting te geven op de defensie-inspanningen inzake cyber.

Werklunch en werksessie

Rapportages over de lastenverdeling

De lastenverdeling stond centraal tijdens de speciale bijeenkomst van staatshoofden en regeringsleiders op 25 mei jl. (Kamerstuk 28 676, nr. 273).
De bondgenoten hebben afgesproken jaarlijks in korte rapportages toe te lichten:

1. hoe zij van plan zijn hun defensie-uitgaven te verhogen in de richting van 2 procent BBP en een investeringsquote van 20 procent te bereiken;
2. in welke mate additionele financiële middelen zullen worden gebruikt om capaciteiten aan te schaffen waar de Navo om vraagt;
3. welke bijdragen aan missies en operaties binnen en buiten Navo-kader zij voor ogen hebben in het komende kalenderjaar.

kst-28676-274
ISSN 0921 - 7371
's-Gravenhage 2017

Aan de hand van korte en zo uniform mogelijke rapportages zullen de bondgenoten deze informatie aanleveren. Dit maakt het mogelijk om de *input* en *output* van de individuele bondgenoten goed te vergelijken.

De nationale informatie moet uiterlijk eind 2017 worden aangeboden, en zal berusten op de begroting voor 2018. Nederland zal met de Navo in overleg treden om de nationale informatie ook aan uw Kamer te kunnen verstrekken. Uiteraard zal Nederland er op aandringen dat ook de andere bondgenoten hun informatie publiek maken.

Follow-on forces

De afgelopen jaren heeft de Navo militaire maatregelen genomen ten behoeve van een geloofwaardige afschrikking. De *NATO Response Force* (NRF) is uitgebreid, binnen de NRF is een *Very High Readiness Joint Task Force* (VJTF) opgericht en sinds begin 2017 is er een vooruitgeschoven Navo-aanwezigheid (*enhanced forward presence*) in de Baltische staten en Polen. De Navo is daarmee in staat onmiddellijk te reageren op een schending van het verdragsgebied.

Voor de geloofwaardige afschrikking en de verdediging van het verdragsgebied is het van belang dat de Navo ook in staat is de ontplooide NRF en de nationale strijdkrachten van een bedreigde bondgenoot snel te versterken. Hiertoe moet de Navo kunnen beschikken over grote eenheden (op land een divisie of groter), de zogenoemde *follow-on forces*. Omdat slechts enkele bondgenoten over eenheden van dergelijke omvang beschikken, is het van belang dat multinationale verbanden geregeld samen trainen. Zo wordt verzekerd dat de *follow-on forces* interoperabel en inzetbaar zijn.

Nederland is voorstander van het integreren en trainen van grotere verbanden. Ons land heeft op dit gebied al stappen gezet. De 43ste Gemechaniseerde Brigade en de 11de Luchtmobiele Brigade zijn al geïntegreerd in respectievelijk de Duitse *1. Panzerdivision* en de *Division Schnelle Kräfte*. Ook hebben Nederland en Duitsland al commandovoeringoefeningen op divisieniveau en legerkorpsniveau uitgevoerd.

Afschrikkingscommunicatie

De ministers zullen aandacht besteden aan de afschrikkingscommunicatie. Geloofwaardige afschrikking vraagt om gerichte boodschappen en acties die onderstrepen dat de Navo de vastberadenheid en capaciteit heeft om op alle dreigingen te reageren. Het is van belang dat de Navo proactief is en tijdig besluiten neemt over de gewenste reactie op de activiteiten van potentiële tegenstanders. Zo wordt verzekerd dat de bondgenoten met één stem spreken en de Navo passende maatregelen kan nemen om de afschrikking geloofwaardig te houden in steeds wijzigende veiligheidsomstandigheden

EU-Navo samenwerking

De ministers zullen tevens spreken over de voortgang van de samenwerking tussen de EU en de Navo. Op 6 december 2016 stemden de EU-lidstaten en de Navo-bondgenoten in met een lijst van 42 voorstellen (Kamerstuk 28 676, nr. 262). Conform afspraak worden de ministers halfjaarlijks ingelicht. De EU-ministers van Buitenlandse Zaken spreken tijdens de Raad Buitenlandse Zaken van 19 juni a.s. ook over de EU-Navo samenwerking.

Inmiddels zijn stappen gezet om de EU-Navo samenwerking verder te verdiepen. De staven van beide organisaties hebben dagelijks contact. De *EU Hybrid Fusion Cell* en de *NATO Hybrid Analysis Cell* werken nauw samen aan het opbouwen van gezamenlijke kennis over hybride dreigingen. Voorts zal in het najaar de eerste gezamenlijke oefening worden georganiseerd. De EU zal deelnemen aan de *Crisis Management Exercise 2017* (CMX17) van de Navo. Volgend jaar zal de Navo naar verwachting deelnemen aan de crisismanagementoefening van de EU. Tot slot werken de EU en de Navo meer samen op het gebied van capaciteitsopbouw in partnerlanden, waaronder Bosnië en Herzegovina, Moldavië en Tunesië. De activiteiten op het gebied van onder meer cyberveiligheid, goed bestuur en veilige munitieopslag in deze landen worden nauw gecoördineerd.

Nederland vindt het positief dat er stappen zijn gezet op het gebied van de EU-Navo samenwerking. Wat Nederland betreft, vormen de 42 voorstellen daarover het beginpunt. Ook is het van belang om concrete vervolgstappen te zetten, bijvoorbeeld op het gebied van het grensoverschrijdende transport van militair materieel en personeel. In de huidige veiligheidsomgeving moeten de Navo en de EU in staat zijn snel te reageren op dreigingen. Eenheden moeten zich snel kunnen verplaatsen naar een inzetgebied. Er bestaan echter nog altijd administratieve obstakels die snelle verplaatsingen belemmeren. Nederland pleit voor nauwe EU-Navo samenwerking in dezen om obstakels weg te nemen, bijvoorbeeld door de ontwikkeling van vereenvoudigde aanvraagprocedures voor vergunningen. Uiteindelijk moet in Europa een «militair Schengengebied» ontstaan, waarbinnen militair materieel en personeel zeer snel kunnen worden verplaatst.

Navo-commandostructuur

In februari jl. hebben de ministers geconcludeerd dat de Navo-commandostructuur (NCS) in de huidige veiligheidsomgeving slechts ten dele in staat is alle noodzakelijke taken goed uit te voeren (Kamerstuk 28 676, nr. 264). De ministers hebben de strategische commandanten van de Navo (de *Supreme Allied Commander Europe* en de *Supreme Allied Commander Transformation*) opdracht gegeven opties uit te werken voor een aangepaste commandostructuur. Een klein comité van deskundigen is hierbij betrokken, waarin ook de voormalige hoofddirecteur Algemene Beleidszaken van Defensie, de heer Lo Casteleijn, zitting heeft.

De strategische commandanten ontwikkelen thans opties. Zij zullen tijdens de ministeriële bijeenkomst hun vorderingen toelichten. In oktober 2017 zullen zij vervolgens hun voorstellen voor een aangepaste commandostructuur presenteren. Nederland zal er op toezien dat niet wordt getornd aan de locatie van het *Joint Forces Command Brunssum*.

Terrorismebestrijding

De ministers zullen spreken over de rol van de Navo bij terrorismebestrijding. Tijdens de speciale bijeenkomst op 25 mei jl. stemden de staatshoofden en regeringsleiders in met een Navo-actieplan voor terrorismebestrijding. Naast de uitbreiding van de inzet van AWACS-radarvliegtuigen ten behoeve van de anti-ISIS coalitie en de toetreding van de Navo tot deze coalitie bevat dit plan onder meer voorstellen voor een grotere Navo-rol op het gebied van capaciteitsopbouw van de veiligheidssector in partnerlanden, zoals Irak en Jordanië. De financiering van dergelijke activiteiten vormt thans nog een punt van discussie. Nederland acht het van belang dat er duidelijke afspraken worden

gemaakt. Zo wordt verzekerd dat het bondgenootschap partnerlanden structureler kan ondersteunen.

Resolute Support missie

De recente aanslagen in Kaboel bevestigen dat de veiligheidssituatie in Afghanistan nog altijd fragiel is. De Afghaanse veiligheidstroepen boeken vooruitgang, maar van volledige zelfstandigheid zal voorlopig nog geen sprake zijn. Het is daarom van belang dat de Navo de Afghaanse veiligheidstroepen blijft trainen en adviseren.

De ministers zullen spreken over de vulling en vormgeving van de *Resolute Support* missie. Het ligt in de rede dat de bondgenoten wordt gevraagd een additionele bijdrage te leveren aan de missie, zodat de huidige troepentekorten kunnen worden aangepakt. Nederland heeft op 24 mei jl. een formeel politiek verzoek van de Verenigde Staten ontvangen om de bijdrage aan de *Resolute Support* missie te continueren en te intensiveren. Het kabinet zal serieus kijken naar de mogelijkheden en heeft een positieve grondhouding ten aanzien van een voortgezette Nederlandse betrokkenheid bij de *Resolute Support* missie na 2017. De Nederlandse bijdrage moet echter in samenhang worden bezien met de overige inzet van de krijgsmacht in EU, Navo, VN en coalitieverband.

Nuclear Planning Group

Voorafgaand aan de ministeriële bijeenkomst vergadert de *Nuclear Planning Group.* De ministers spreken over het nucleaire beleid van de Navo.

De Minister van Defensie,
J.A. Hennis-Plasschaert

BIJLAGE:

DEFENSIE-INSPANNINGEN OP CYBERGEBIED

Defensie Cyber Strategie

Defensie ontplooit en ontwikkelt sinds 2012 cyberactiviteiten en -capaciteiten aan de hand van de Defensie Cyber Strategie. De investeringen richten zich vooral op het verhogen van de digitale weerbaarheid, het versterken van het inlichtingenvermogen en het ontwikkelen van offensieve cybercapaciteiten. Sinds 2015 investeert Defensie aanvullend in cybermiddelen.

De geactualiseerde Cyber Strategie van februari 2015 (Kamerstuk 33 321, nr. 5) besteedt specifiek aandacht aan de voorwaarden voor succes in het cyberdomein. Belangrijke elementen zijn het omgaan met en inspelen op kort-cyclische, «kleinschalige» innovaties, het boeien en binden van cyberprofessionals en de samenwerking binnen Defensie en met partners in het binnen- en buitenland.

Met de voortgangsrapportage van 15 maart 2016 (Kamerstuk 33 321, nr. 7) is uw Kamer geïnformeerd over de uitvoering van de Defensie Cyber Strategie. Aan het begin van deze kabinetsperiode is besloten tot een versnelling van de ontwikkeling van cybercapaciteiten bij Defensie. Dit heeft onder meer geleid tot de oprichting van de *Joint Sigint Cyber Unit* (JSCU) van de MIVD en AIVD en het Defensie Cyber Commando (DCC).

Defensief

Het Defensie *Computer Emergency Response Team* (DefCERT) van het Joint IV Commando (JIVC) waakt over de veiligheid van de netwerken en systemen van Defensie en adviseert en ondersteunt bij cyberincidenten. DefCERT heeft een samenwerkingsovereenkomst met het Nationaal Cyber Security Centrum (NCSC) van de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) en werkt intensief samen met CERT's van andere landen, de Navo en het bedrijfsleven.

Ook richt Defensie thans een *Security Operations Centre* (SOC) op, waarin de beheersorganisaties samenwerken om alle netwerken, IT-diensten en sensoren, wapensystemen en commandosystemen van Defensie dag en nacht te monitoren en te beschermen. Dit SOC krijgt extra personeel tot zijn beschikking en zal nauw samenwerken met DefCERT.

Inlichtingen

De dreiging van digitale spionage tegen Defensie, toeleveranciers, bondgenootschappelijke netwerken en producenten van militair-relevante producten is aanzienlijk. Deze dreiging neemt in omvang toe, wordt steeds agressiever en geavanceerder en is vanuit het perspectief van aanvallers ongeëvenaard succesvol. Waar buitenlandse inlichtingendiensten voorheen vooral gebruikmaakten van agenten, kan tegenwoordig veelal worden volstaan met een handeling vanaf een anonieme computer. Aanvallen van statelijke actoren worden doorgaans niet gedetecteerd door commerciële producten. Daarom doet de MIVD hiernaar zelf actief onderzoek. De MIVD detecteert, analyseert digitale aanvallen en digitale spionage en beschikt over het vermogen om inlichtingenactiviteiten van anderen tegen Defensie te verstoren en te stoppen. De versterking van het cyber-inlichtingenvermogen betreft vooral het vermogen te infiltreren in systemen en het verwerven van cyberinlichtingen met het oog op (potentiële) militaire operaties. Een deel van deze investering is ondergebracht bij de JSCU van de MIVD en de AIVD.

De onderzoeken komen ook de verdediging van de defensienetwerken ten goede. Door de deelneming van de MIVD aan het Nationaal Detectie Netwerk (NDN) levert Defensie ook een bijdrage aan de bescherming van de rijksoverheid en het bedrijfsleven.

Offensief

Het Defensie Cyber Commando ontwikkelt in nauwe samenwerking met onder meer de MIVD en DefCERT het militaire vermogen om (offensieve) cyberoperaties uit te voeren. Een doctrine voor het optreden in het digitale domein is thans in ontwikkeling. Deze zal onder andere ingaan op het verder integreren van cybermiddelen in de operationele planning van militaire operaties.

Samenwerking

Defensie werkt intensief samen met het Ministerie van Veiligheid en Justitie en andere departementen, onder andere door deel te nemen aan de Cyber Security Raad en het NCSC. Defensie heeft een liaison in het NCSC en zowel DefCERT als de MIVD hebben afspraken met het NCSC over wederzijdse ondersteuning en bestendiging van de samenwerking. De MIVD werkt nauw samen met de AIVD op cybergebied in de JSCU.

Defensie werkt ook intensief samen met publieke en private partijen binnen het cyberdomein. In internationaal verband werkt Defensie onder andere samen in de Navo en de EU. Over deze samenwerking heeft u op 5 juli 2016 een brief ontvangen (Kamerstuk 33 321, nr. 8).

Ook de samenwerking met het bedrijfsleven staat hoog op de agenda. Het bedrijfsleven is een belangrijke aanjager van kennisontwikkeling en innovatie in het digitale domein. Gezamenlijke onderzoeksprogramma's, de ontwikkeling van capaciteiten en samenwerking bij opleidingen en trainingen staan hierbij centraal. Deze samenwerkingsvormen kunnen de ontwikkeling van de verschillende digitale middelen bij Defensie belangrijke impulsen geven.