Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

33 321 Defensie Cyber Strategie

Nr. 9 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 november 2018

Hierbij stuur ik u de nieuwe Defensie Cyber Strategie[1], zoals aangekondigd in de Defensienota (Kamerstuk 34 919, nr. 1, 26 maart 2018). Met deze strategie voer ik eveneens de motie Bruins Slot c.s. over investeringen in cyber als volwaardig vijfde militaire domein en een grotere rol van Defensie in het kader van de derde hoofdtaak (Kamerstuk 34 775 X, nr. 40, 23 november 2017) en de motie Diks over de capaciteit van het Defensie Cyber Commando en de inzet van cybercapaciteiten in het kader van de internationale rechtsorde (Kamerstuk 34 919, nr. 11, 28 mei 2018) uit.

In het Regeerakkoord *Vertrouwen in de toekomst* (10 oktober 2017, bijlage bij Kamerstuk 34 700, nr. 34) is vastgesteld dat een versterking van de rol van Defensie in de digitale beveiliging en bewaking van Nederland vanuit zijn grondwettelijke verantwoordelijkheid nodig is. De verslechtering van de internationale veiligheidscontext geeft hier ook alle aanleiding toe. We zien op bijna dagelijkse basis hoe het digitale domein wordt misbruikt voor geopolitieke doeleinden.

Nederland blijft actief inzetten op bestendiging van het internationaal recht in het digitale domein. Daarnaast versterken we ook onze digitale slagkracht (zie ook de Nederlandse Cybersecurity Agenda (NCSA) Kamerstuk 26 643, nr. 536, 20 april 2018). Nederland moet, al dan niet in coalitieverband, in staat zijn onverwijld en adequaat te reageren op digitale dreigingen, zoals cyberaanvallen door statelijke actoren. Hiertoe werken we, in lijn met de Defensienota en de Geïntegreerde Buitenland- en Veiligheidsstrategie (Kamerstuk 33 694, nr. 12, 19 maart 2018), onder andere aan onze offensieve slagkracht, die een bijdrage levert aan het vermogen tot afschrikking van cyberaanvallen. Ook dragen we zo bij aan het handelingsvermogen in NAVO- en EU-verband in het digitale domein.

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-33321-9
ISSN 0921 - 7371
's-Gravenhage 2018

Naast offensieve capaciteiten draagt ook een actief attributiebeleid bij aan het afschrikken van cyberaanvallen. Door de actoren achter een cyberaanval (publiekelijk) te identificeren willen we de straffeloosheid in het cyberdomein terugdringen. Het aanwijzen van de Russische inlichtingendienst GRU als verantwoordelijke voor de hackpoging tegen de OPCW in Den Haag is hiervan een recent voorbeeld (Kamerstuk 33 694, nr. 21, 4 oktober 2018). Een actief attributiebeleid draagt bij aan het minder aantrekkelijk worden van Nederland als doelwit van cyberaanvallen.

Bij de in het regeerakkoord aangekondigde versterking van de rol van Defensie bij de verdediging van Nederland in het digitale domein, richten we ons met name op de vitale infrastrucuur. Staten voeren digitale aanvallen uit op andere landen en organisaties, met als doel onder andere (toekomstige) verstoring of sabotage van vitale systemen (Cyber Security Beeld Nederland 2018, Kamerstuk 26 643, nr. 540, 13 juni 2018). Dit kan maatschappijontwrichtende gevolgen hebben. Die kans is zeker bij internationale crises niet denkbeeldig. In nauwe samenwerking met de NCTV wordt de komende tijd uitgewerkt hoe de cybercapaciteiten van Defensie ingezet kunnen worden om de digitale veiligheid van Nederland en van onze vitale infrastructuur te helpen waarborgen.

Tot slot blijft de weerbaarheid van onze eigen (wapen)systemen en netwerken onveranderd belangrijk, zeker in de context van de toenemende digitale dreiging.

Over deze en andere maatregelen gaat de Defensie Cyber Strategie. Defensie zal zich met haar partners de komende jaren onverminderd inzetten om nationale en internationale veiligheid en stabiliteit te bevorderen, ook in het digitale domein. Digitale slagkracht legt daarvoor de basis.

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten