Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019 **Aanhangsel van de Handelingen**

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

1236

Vragen van het lid **Bruins Slot** (CDA) aan de Minister van Defensie over *een onzichtbaar cyberleger* (ingezonden 27 december 2018).

Antwoord van Minister **Bijleveld-Schouten** (Defensie) (ontvangen 21 januari 2019).

Vraag 1
Heeft u kennisgenomen van het bericht «Het cyberleger is er wel, maar mag weinig»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat het Defensie Cyber Commando (DCC) in plaats van de nagestreefde 200 militairen slechts met 80 tot 100 militairen gevuld is? Zo ja, vindt u hiervan en wat gaat u hieraan doen?

Antwoord 2
Een formatie van 200 personen is geen specifiek streven van het DCC. Het kabinet heeft 95 miljoen euro extra geïnvesteerd in cybersecurity, waarvan 20 miljoen voor Defensie. Van dit bedrag wordt een aanzienlijk deel geïnvesteerd in personele versterking van het DCC.

Vraag 3
In hoeverre bestaat er onduidelijkheid over wat het commando precies kan, mag en wil? Zo ja, op welke onderwerpen bestaat die onduidelijkheid?

Antwoord 3
Over de inzet van het DCC is geen onduidelijkheid. Net als de offensieve inzet van elk militair middel, geldt dat daarvoor een politiek besluit tot inzet nodig is, waarbij een mandaat en «rules of engagement» worden vastgesteld. Dit kan in het kader van expeditionaire inzet van de krijgsmacht, alsook in geval van verdediging van ons land of ons bondgenootschappelijk grondgebied, in overeenstemming met het internationaal recht.

[1] https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254

ah-tk-20182019-1236
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 4
Herkent u zich in de kritiek van onderzoekers dat het vermogen om hoogwaardige doelen uit te schakelen nog niet aanwezig is en dat de budgetten tekortschieten?

Antwoord 4
De bruikbaarheid van onze cybercapaciteiten is, zoals voor al onze capaciteiten geldt, volledig afhankelijk van de context waarin de krijgsmacht wordt ingezet. Om op voorhand te stellen dat het DCC per definitie niet in staat is hoogwaardige doelen aan te grijpen, is ongefundeerd.

Vraag 5
Klopt het dat het Amerikaanse cybercommando websites van terreurorganisatie ISIS met propagandamateriaal weg heeft gehaald en het de toegang van cyberpropagandisten van ISIS tot social media accounts heeft geblokkeerd?

Antwoord 5
In openbare bronnen, zoals de verslagen van gesprekken van de Amerikaanse Senaat met de commandant van het USCYBERCOM, wordt uitgebreid verslag gedaan van de bijdrage van het Amerikaanse cyber commando aan de strijd tegen ISIS. Hierin valt te lezen dat dit onder andere de vernietiging van de online propaganda-infrastructuur van ISIS behelst.

Vraag 6
Mag het DCC soortgelijke operaties uitvoeren? Zo nee, waarom niet?

Antwoord 6
Het mandaat voor de inzet van digitale middelen door de krijgsmacht wordt per militaire missie of operatie vastgesteld. De bestaande volkenrechtelijke regels inzake het gebruik van geweld zijn van toepassing op digitale aanvallen.

Vraag 7
Is het waar dat cybersoldaten van het DCC elders worden gedetacheerd? Hoe vaak gebeurt dit? Wat is de reden hiervan?

Antwoord 7
Ja, dit gebeurt met enige regelmaat, met name bij de MIVD. Zoals uitgelegd in onder andere de Defensie Cyber Strategie, komen de benodigde kennis en vaardigheden voor het uitvoeren van offensieve cyberoperaties sterk overeen met die voor het uitvoeren van digitale inlichtingenoperaties. Door middel van detacheringen over en weer tussen verschillende defensieonderdelen die in het cyberdomein opereren, versterken we defensiebreed onze cybervaardigheden.

Vraag 8
Klopt het dat de vorige commandant van het DCC de strijd verloor om het cybercommando een rol te laten spelen bij de bescherming van de Rotterdamse haven, de digitale bescherming van kerncentrales en andere mogelijke doelwitten? Zo ja, wat is de reden hiervan?

Antwoord 8
Van strijd om de verdediging van vitale infrastructuur is geen sprake. Om Nederland digitaal veilig te houden wordt op gecoördineerde wijze samengewerkt door zowel publieke als private organisaties. In het regeerakkoord is vastgelegd dat Defensie een grotere rol gaat spelen bij de digitale beveiliging en bewaking van Nederland. In de Defensie Cyber Strategie heb ik uitgelegd dat Defensie zich hierbij, onder coördinatie van de NCTV, specifiek gaat richten op de vitale infrastructuur.

Vraag 9, 10
Welke bijdrage levert het DCC aan het bereiken van de doelstellingen in de recent uitgebrachte Defensie Cyber Strategie 2018? Waarom wordt het DCC nauwelijks in de Defensie Cyber Strategie 2018 genoemd?
Hoe verhoudt zich een en ander tot de doelstelling in de Defensienota om één defensieve en/of offensieve cyberoperatie uit te voeren, alsmede de

motie Bruins Slot c.s.[2] over investeringen in cyber als volwaardig vijfde militair domein en een grotere rol voor Defensie in het kader van de derde hoofdtaak en de motie Diks[3] over de capaciteit van het Defensie Cyber Commando en de inzet van cybercapaciteiten in het kader van de internationale rechtsorde?

Antwoord 9, 10
Het DCC levert een belangrijke bijdrage aan het realiseren van de doelstellingen van de Defensie Cyber Strategie. Het kabinet heeft 95 miljoen euro extra geïnvesteerd in cybersecurity, waarvan 20 miljoen voor Defensie. Van dit bedrag wordt een aanzienlijk deel geïnvesteerd in personele versterking van het DCC. Door te investeren in de capaciteiten van het DCC werken we aan een krijgsmacht die effectief inzetbaar is in het digitale domein. Ook wordt door het ontwikkelen van geloofwaardige, offensieve digitale capaciteiten van het DCC, bijgedragen aan de afschrikkingsfunctie van de krijgsmacht. Nederland heeft zich bereid verklaard om waar nodig en mogelijk met digitale capaciteiten bij te dragen aan NAVO-missies en -operaties.
Tot slot gaat Defensie de uitvoering van de derde hoofdtaak in het digitale domein versterken door een grotere bijdrage te leveren aan bestaande civiele structuren. Vraag en aanbod van cybercapaciteiten van Defensie worden in overleg met de civiele autoriteiten en betrokken publieke en private partners in kaart gebracht. Gezien de aard van de dreigingen richt Defensie zich daarbij met name op de vitale infrastructuur door intensievere samenwerking met de daartoe bij wet aangewezen organisaties, met name het Nationaal Cyber Security Centre.

[2] Kamerstuk 34 775 X, nr. 40
[3] Kamerstuk 34 919, nr. 11