Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

2140

Vragen van de leden **Haverkamp** en **Knops** (beiden CDA) aan de ministers van Buitenlandse Zaken en van Defensie over *cyberaanvallen* (ingezonden 11 maart 2010).

Antwoord van minister **Verhagen** (Buitenlandse Zaken) en minister **Van Middelkoop** (Defensie) (ontvangen 6 april 2010).

Vraag 1
Bent u bekend met het artikel in The Times «Cyberwar declared as China hunts for the West's intelligence secrets»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u aangeven in hoeverre de constatering in het artikel waar is, dat het aantal cyberaanvallen op NAVO-bondgenoten de afgelopen 12 maanden fors is toegenomen en dat China hierin één van de meest actieve spelers is? Kunt u aangeven in hoeverre dit heeft geleid tot een beperking van het functioneren van veiligheidsdiensten?

Antwoord 2
Digitale aanvallen op netwerken en organisaties nemen toe, ook vanuit China. Overigens is de aard van de dreiging veelvormig en de herkomst niet altijd vast te stellen.
Over het functioneren van veiligheidsdiensten worden in het openbaar geen mededelingen gedaan.

Vraag 3
Is de constatering juist dat Amerikaanse en Britse systemen beter tegen deze aanvallen beschermd zijn dan systemen van andere Europese bondgenoten binnen de NAVO en dat goede samenwerking en uitwisseling van informatie wordt bemoeilijkt doordat Europese veiligheidssystemen van lager niveau zijn dan die van de VS en Groot-Brittannië? Zo ja, welke stappen zouden de Europese bondgenoten volgens u moeten zetten om betere samenwerking mogelijk te maken?

[1] Times Online, 8 maart 2010.

ah-tk-20092010-2140
ISSN 0921 - 7398
's-Gravenhage 2010

Antwoord 3
Binnen de NAVO worden aan informatiesystemen zowel op het gebied van beveiliging als ten aanzien van de interoperabiliteit eisen gesteld. Hiermee is een gemeenschappelijk beveiligingsniveau vastgesteld dat door de NAVO voldoende wordt geacht als bescherming tegen aanvallen. Deze eisen zijn bindend voor alle informatiesystemen van de lidstaten en garanderen een goede onderlinge informatie-uitwisseling.

Vraag 4 en 5
Deelt u de mening dat binnen de NAVO, conform artikel 4 van het NAVO-verdrag, moet worden gezocht naar mogelijkheden om de digitale veiligheid van alle bondgenoten te versterken? Zo nee, waarom niet?
Deelt u de mening dat in het nieuwe Strategische Concept van de NAVO expliciet aandacht moet worden besteed aan de bescherming van de bondgenoten tegen cyberaanvallen en de manier waarop op dit gebied kan worden samengewerkt? Zo nee, waarom niet? Zo ja, op welke manier zult u dit in de lopende discussie over het nieuwe Strategisch Concept bevorderen?

Antwoord 4 en 5
De NAVO-top in Boekarest heeft ingestemd met het beleid inzake cyber aanvallen, zoals dat in reactie op de cyber aanvallen op Estland in 2007 verder is ontwikkeld. Op grond van dit beleid is onder meer de samenwerking met het in Estland gevestigde *Cooperative Cyber Defence Centre of Excellence versterkt*.
Het Strategisch Concept zal het belang van bescherming tegen cyber aanvallen expliciet moeten onderkennen. Zoals in de regeringsreactie van 31 maart jl. op het AIV-advies over het NAVO Strategisch Concept aan u is gemeld, delen wij de mening dat artikel 4 beter moet worden benut om over nieuwe dreigingen als cyber aanvallen binnen het bondgenootschap te spreken. Het Strategisch Concept zal tevens duidelijk moeten maken dat de samenwerking met andere organisaties, in het bijzonder de EU, op dit terrein is geboden. De regering heeft haar inzet op deze en andere punten gedeeld met de Groep van Experts tijdens consultaties met de vertegenwoordiger van de Groep, in de persoon van Jeroen van der Veer.

Vraag 6
Kunt u ingaan op de uitvoering van de motie-Knops c.s.[2], waarin wordt gevraagd om de ontwikkeling in interdepartementaal verband van een cyber security strategie en de actieve bijdrage aan de gedachtevorming binnen de NAVO op dit onderwerp, waarover de Kamer uiterlijk 1 maart 2010 zou worden geïnformeerd?

Antwoord 6
Hiervoor wordt u verwezen naar de brief van de minister van Defensie van 11 maart jl.

[2] Kamerstuk 32 123 X, nr. 66.