Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

Aanhangsel van de Handelingen

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

2612

Vragen van het lid **Van Raak** (SP) aan de ministers van Veiligheid en Justitie en van Defensie over *de aanpak van cyberspionage* (ingezonden 8 april 2011).

Antwoord van ministers **Opstelten** (Veiligheid en Justitie) en **Hillen** (Defensie) (ontvangen 24 mei 2011).

Vraag 1 t/m 4
Waarom gaat het ministerie van Defensie 90 miljoen euro investeren in de bestrijding van digitale aanvallen, terwijl tegelijkertijd het ministerie van Veiligheid en Justitie een Nationaal Cyber Security Centrum gaat oprichten?[1]
Wat zijn de verschillen in aanpak van cyberaanvallen van u beide?
Wie van u beide heeft uiteindelijk de regie over de aanpak van cyberspionage?
Waarom is niet gekozen voor één organisatie die verantwoordelijk wordt voor het opsporen en aanpakken van cyberaanvallen?

Antwoord 1 t/m 4
De genoemde activiteiten van de ministeries van Veiligheid en Justitie en Defensie op het terrein van *cyber security* zijn complementair. De minister van Veiligheid en Justitie voert, in lijn met de uitgangspunten van de Strategie Nationale Veiligheid, de regie op de samenhang en samenwerking ten aanzien van het vergroten van de *cyber security*.
De aanpak van een dreiging in het digitale domein geschiedt op grond van verschillende bevoegdheden onder verantwoordelijkheid van meerdere departementen en instanties. Naast de ministeries van Veiligheid en Justitie en Defensie gaat het hierbij onder meer om het ministerie van Economie, Landbouw en Innovatie, GOVCERT (het c*yber security* en *incident response team* van de overheid), het KLPD en de inlichtingen- en veiligheidsdiensten. Verder zetten ook private organisaties (o.a. leveranciers van hard- en software en internet providers) en internationale organisaties (EU en NAVO) zich in om Nederland op grond van specifieke verantwoordelijkheden weerbaarder te maken tegen cyberaanvallen.
In het Nationaal Cyber Security Centrum krijgen deelnemende publieke en private organisaties beter zicht op kwetsbaarheden, dreigingen, ontwikkelingen en trends zodat zij maatregelen kunnen treffen om de veiligheid en betrouwbaarheid van de nationale ICT infrastructuur te verbeteren. Daarnaast zullen in de Cyber Security Raad afspraken op strategisch niveau worden

[1] De Telegraaf, donderdag 7 april 2011.

ah-tk-20102011-2612
ISSN 0921 - 7398
's-Gravenhage 2011

gemaakt waardoor de activiteiten van betrokken organisaties elkaar versterken en aanvullen.
Zoals gesteld in de Beleidsbrief van 8 april 2011 (Kamerstuk 32 733, nr.1) zal Defensie, om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, haar digitale weerbaarheid de komende jaren versterken en het vermogen ontwikkelen tot het uitvoeren van *cyber operations*. De cybercapaciteit van Defensie zal gefaseerd worden ontwikkeld. Het zwaartepunt ligt de komende jaren bij het verbeteren van de bescherming van netwerken, systemen en informatie van Defensie en de uitbreiding van de inlichtingencapaciteit in het digitale domein. Voor de periode 2011 to 2015 bedraagt de totale intensivering € 50 miljoen, inclusief de personele exploitatie. De volledige cybercapaciteit zal in 2016 gereed zijn. Daarna bedraagt de intensivering structureel € 21 miljoen.

Vraag 5
Wat gaat u beide doen om de strijdbijl te begraven en te komen tot één aanpak tegen cyberaanvallen?

Antwoord 5
Zoals hierboven gesteld, is er sprake van een gezamenlijke aanpak ter verbetering van de *cyber security*. Op alle niveaus wordt goed samengewerkt om gezamenlijk de ambities van het kabinet ter versterking van de *cyber security* waar te maken.