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

578

Vragen van het lid **Recourt** (PvdA) aan de minister van Veiligheid en Justitie over *de bestrijding van cybercrime* (ingezonden 27 oktober 2010).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) (ontvangen 23 november 2010) Zie ook Aanhangsel Handelingen, vergaderjaar 2010–2011, nr. 453.

Vraag 1
Bent u bekend met de uitzending van Nieuwsuur over cybercrime?[1]

Antwoord 1
Ja.

Vraag 2 t/m 4
Bent u het met een aantal geïnterviewden, waar onder de officier van justitie gespecialiseerd in cybercrime, eens dat de bevoegdheden van politie en justitie moeten worden uitgebreid ten aanzien van cybercrime, meer in het bijzonder de mogelijkheid om «terug te hacken», ongeacht de plaats waar de computer zich bevindt?
Is het waar dat in de uitzending de optredende officier van justitie om een dergelijke wetswijziging heeft verzocht?
Bent u bereid aan dit verzoek te voldoen?

Antwoord 2 t/m 4
De door de officier van justitie in de uitzending geuite wens komt overeen met de in de kader van de consultatieronde ter voorbereiding van het wetsvoorstel Computercriminaliteit III geuite wens van het College van procureurs-generaal om een wettelijke grondslag te creëren voor het binnendringen in en betreden op afstand van een geautomatiseerd werk. Na afloop van de consultatieronde zal ik de daarin naar voren gebrachte punten nader bezien.

Vraag 5
Kunt u een dergelijke bevoegdheidsuitbreiding realiseren binnen de nationale wetgeving? Zo ja, hoe? Zo nee, op welke wijze kunt u op korte en lange termijn deze vorm van grensoverschrijdende criminaliteit effectief aanpakken?

[1] Nieuwsuur, «Strijd tegen cybercrime», 25 oktober 2010.

ah-tk-20102011-578
ISSN 0921 - 7398
's-Gravenhage 2010

Antwoord 5
De bij het antwoord op de vragen 2, 3 en 4 aangehaalde bevoegdheden zijn in beginsel binnen de nationale wetgeving te realiseren. En daartoe zal ik voorstellen doen. Voor de internationale dimensie merk ik op dat veel bevoegdheden nationaal vast te leggen zijn, maar het grensoverschrijdende gebruik ervan mede afhangt van de rechtsmacht die op de opsporing en vervolging van grensoverschrijdende of buiten Nederland plaatsvindende misdrijven gelegd wordt en in hoeverre die door de betreffende staat gelegde rechtsmacht internationaal geaccepteerd wordt. Zoals bekend hanteert Nederland een terughoudend beleid op dit punt.

Vraag 6
Bent u bereid extra opsporings- en vervolgingscapaciteit in te zetten voor dit soort misdaad?

Antwoord 6
In het kader van het programma versterking aanpak cybercrime zijn reeds extra gelden beschikbaar gesteld, waarmee opsporing en vervolging een nieuwe impuls hebben gekregen. Ook binnen de bestaande middelen van het OM en de politie zijn aanpassingen gedaan om te voldoen aan de eisen die voortkomen uit de ontwikkelingen in de cybercrime.

Vraag 7
Is er voldoende kennis en kunde aanwezig op dit terrein bij justitie en politie?

Antwoord 7
Het kennisniveau bij gespecialiseerde afdelingen zoals het Team Hightech Crime en het Team Digitaal & Internet van de Dienst Nationale Recherche van het KLPD is hoog. Nederland staat wereldwijd goed bekend wat betreft de bestrijding van hightech crime. Dat neemt niet weg dat het kennisniveau bij de politie en het Openbaar Ministerie nog in ontwikkeling is. In Nederland is in 2006 een Nationale Infrastructuur Bestrijding Cybercrime opgezet en in 2007 een intensiveringsprogramma ontwikkeld. Het doel van deze maatregelen is, onder andere, het verspreiden en opbouwen van kennis en vaardigheden. Voor de aanpak van bijvoorbeeld phishing en botnets zijn zogenaamde proeftuinen ingericht.