Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Juridische en Operationele Aangelegenheden
2 DJOA

Schedeldoekshaven 100
2511 EX Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

**Ons kenmerk**
295619

**Uw kenmerk**
2012Z15029

*Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.*

Datum 24 augustus 2012
Onderwerp Beantwoording Kamervragen over het bericht dat Nederland moet terughacken

In antwoord op uw brief van 13 augustus 2012 deel ik u mede dat de schriftelijke vragen van de leden Hachchi en Schouw (beiden D66) over het bericht dat Nederland moet terughacken (ingezonden 13 augustus 2012) worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Juridische en Operationele Aangelegenheden
2 DJOA

**Datum**
24 augustus 2012

**Ons kenmerk**
295619

**Vragen van de leden Hachchi en Schouw (beiden D66) aan de minister van Veiligheid en Justitie over het bericht dat Nederland moet terughacken (ingezonden 13 augustus 2012, 2012Z15029)**

---

Vraag 1
**Bent u bekend met het bericht "Nederland moet 'terughacken'"?**

Antwoord
Ja.

**Vraag 2**
**Welke acties onderneemt u precies als buitenlandse servers virussen in ons land verspreiden?**

Antwoord
In eerste instantie is het niet een verantwoordelijkheid van de overheid, maar van een ieder die met een computer het internet op gaat of op andere wijze met computers werkt om zijn eigendommen te beschermen. Hiervoor is een groot aantal computertools beschikbaar. Ook internetserviceproviders ondersteunen gebruikers bij het voorkomen van virusuitbraken.
Voor de overheid geldt dat zij, mede gezien haar verantwoordelijkheid voor de veiligheid van de dienstverlening aan burgers, de nodige maatregelen moet treffen om haar eigen infrastructuur vrij te houden van virussen. Daarnaast verstrekt de overheid op diverse manieren voorlichting. Bij bijzondere dreigingen en incidenten, zoals bij de aanpak van het Dorifel-virus, kan een grotere inzet van de overheid aan de orde zijn. Het Nationaal Cyber Security Centrum (NCSC) speelt dan een rol door het bijeenbrengen en uitdragen van informatie en expertise, en door het bieden van handelingsperspectieven. Wanneer sprake is van een acute dreiging, kan worden voorzien in tijdige en adequate alertering, zodat partijen zelf hun voorbereidingen kunnen treffen en verantwoordelijkheid kunnen nemen.

**Vraag 3**
**Wat houdt "terughacken" precies in?**

Antwoord
De term terughacken is niet afkomstig van de overheid. Door het NCSC wordt hacken gedefinieerd als het intrekken in computersystemen. Vanuit deze redenering is terughacken het inbreken in computersystemen van waaruit gehackt wordt met als doel om de oorspronkelijke dreiging te doen stoppen.

**Vraag 4**
**Wat is uw reactie op de uitspraak dat Nederland te soft optreedt en dat Nederland moet "terughacken"?**

**Vraag 5**

**Behoort volgens u "terughacken" tot de mogelijkheden om servers die virussen verspreiden uit te schakelen? Kunt u dit toelichten?**

**Vraag 6**
**Welke consequenties heeft het "terughacken"?**

**Vraag 7**
**Wat zijn de risico's van het "terughacken" zowel op korte als op lange termijn?**

**Vraag 8**
**Welke (juridische) waarborgen zijn volgens u noodzakelijk om het "terughacken" van landen mogelijk te maken?**

Antwoord 4 t/m 8
Nederland handelt binnen de eigen wettelijke kaders. Via de samenwerking met andere landen, die mede is vormgegeven door het Cybercrimeverdrag, zijn in veel gevallen bedreigingen af te wenden. Wel constateer ik dat in de snel veranderende digitale wereld de wetgeving en internationale afspraken zijn achter gebleven. Om die reden heb ik uw Kamer laten weten dat ik met voorstellen zal komen met als doel het juridisch kader voor de opsporing en vervolging van cybercrime meer toe te snijden op de behoeften van de diensten die zijn belast met de opsporing en vervolging van cybercrime. In het kader van dat wetstraject zal ik ook uitgebreider ingaan op de consequenties en risico's van terughacken. Tot slot verwijs ik u naar mijn antwoorden op de vragen van het lid Recourt over de bestrijding van cybercrime (Aanhangsel Handelingen, vergaderjaar 2010-2011, nr. 578).

**Vraag 9**
**Wat vindt u van het voorstel om te pleiten voor internationale afspraken voor internet, vergelijkbaar met het internationale zeerecht? Welke juridische consequenties heeft dit?**

Antwoord 9
Het is duidelijk dat er behoefte is aan nieuwe regels voor de grensoverschrijdende bestrijding en voorkoming van cybercrime. Daarover vindt wereldwijd volop discussie plaats. Ook op Europees niveau wordt gezocht naar oplossingen. Een fundamenteel onderdeel van deze discussie is het territorialiteitsbeginsel en het uitgangspunt van nationale soevereiniteit. Dat ligt in veel landen erg gevoelig. De lopende discussies overziend constateer ik dat we inhoudelijk nog niet zo ver zijn dat concrete oplossingen in zicht komen. Het voorstel dat de oplossing is gelegen in de mogelijke vergelijking met het internationale zeerecht is dan ook interessant, maar prematuur.

1) http://nos.nl/artikel/405160-nederland-moet-terughacken.html

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Juridische en Operationele Aangelegenheden
2 DJOA

**Datum**
24 augustus 2012

**Ons kenmerk**
295619