Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

210

Vragen van het lid **Oosenbrug** (PvdA) aan de Minister van Veiligheid en Justitie over *het bericht dat hackers boos zijn vanwege criminalisering door het Openbaar Ministerie(OM)* (ingezonden 27 augustus 2014).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 9 oktober 2014) Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 36

Vraag 1
Kent u het bericht «Hackers boos om «criminalisatie» door OM»[1], kent u de in het bericht genoemde aan u gestuurde open brief van bestuursleden van elf hackersgroepen[2] en kent u de site van het OM «Uw mening over straffen voor hacken»[3]?

Antwoord 1
Ja.

Vraag 2
Worden mede aan de hand van de antwoorden op vragen van de genoemde site van het OM richtlijnen over straffen aangepast? Zo ja, op welke wijze? Zo nee, waar zijn de antwoorden voor de vragen dan wel voor bedoeld?

Antwoord 2
Bij het maken of aanpassen van strafvorderingsrichtlijnen gebruikt het Openbaar Ministerie (OM) de input van experts, ketenpartners en de samenleving. Het laatste gebeurt door het op diverse plaatsen organiseren van burgerfora en jongerenfora en het plaatsen van een enquête op de site OM.nl. Het OM probeert op die manier vooral te vernemen wat burgers als strafverzwarende omstandigheden zien bij een bepaald delict. De burgerraadpleging over de strafbaarheid van computervredebreuk (artikel 138ab Wetboek van Strafrecht) heeft plaatsgevonden omdat het OM bezig is een strafvorderingsrichtlijn voor dit misdrijf op te stellen.

---

[1] http://www.nutech.nl/internet/3861124/hackers-boos-criminalisatie.html
[2] http://computervrede.nl/2014-08-26-OpenbaarMinisterie/
[3] https://www.om.nl/onderwerpen/mening/virtuele_map/mening-straffen-0/

ah-tk-20142015-210
ISSN 0921 - 7398
's-Gravenhage 2014

Vraag 3 en 4
Deelt u de mening van de bestuursleden van de genoemde hackersgroepen dat «hacken op creatieve wijze meer doen met techniek [is] dan de makers zelf hadden bedacht, het opzoeken van de grenzen van het mogelijke en het verkennen van de ethische en maatschappelijke consequenties van de ontdekte mogelijkheden»? Zo ja, waarom wordt hacken op de site van het OM dan in de context van criminaliteit geplaatst? Zo nee, waarom niet?
In hoeverre wordt hacken in het algemene spraakgebruik gelijk gesteld aan computerhuisvredebreuk of vergelijkbare strafbare feiten door middel van computers? Deelt u de mening dat het algemene spraakgebruik ten aanzien van hacken niet het uitgangspunt voor het bepalen van strafvorderingsrichtlijnen van het OM mag zijn, maar dat daarvoor de juridisch juiste termen dienen te worden gebruikt?

Antwoord 3 en 4
Als voorlichting wordt gegeven, sluit het OM zoveel mogelijk aan bij het taalgebruik en de terminologie zoals die in de maatschappij gangbaar zijn. De term «hacker» heeft daarin een meervoudige betekenis. Enerzijds wordt daarmee gedoeld op de in technologie geïnteresseerde hobbyist of professional die actief de grenzen van de techniek op zoekt of die zich heeft gespecialiseerd in het testen van de beveiliging van computersystemen en -netwerken. Anderzijds wordt de term ook gebruikt voor individuen die zich in strafrechtelijke zin schuldig maken aan (in het bijzonder) computervredebreuk.
Bij de voorlichting over concrete opsporingsonderzoeken naar computervredebreuk is het gebruik van de term «hacker» naar de mening van het OM steeds voldoende duidelijk. In gevallen waarin die context niet duidelijk is spreekt het OM in haar publieke uitingen van «criminele hackers» of «criminelen». Op de OM-site zal door middel van een disclaimer nog uitdrukkelijk worden aangegeven dat hacken in deze betekenis wordt bedoeld. Bij het OM leeft geenszins het idee dat alle hackers criminelen zijn. Integendeel, het OM erkent de meervoudige betekenis van de term en is zich ten volle bewust van de meerwaarde die hackers (in de eerste betekenis van het woord) hebben bij het verhogen van de digitale veiligheid van onze maatschappij. In dat kader treedt het OM ook met regelmaat in gesprek met personen uit de gemeenschap van hackers, onder andere over de vraag waar de grens ligt tussen crimineel hacken en niet-crimineel hacken. Op de in de open brief aangehaalde themadag is het OM bijvoorbeeld met hen in gesprek gegaan over het door het OM (kort daarvoor gepubliceerde) beleid ten aanzien van «responsible disclosure». Het OM gaat ook in de toekomst deze dialoog over hacken graag aan, zonder vooroordelen over de betrokkenheid bij enig strafbaar feit.

Vraag 5 en 6
Deelt u de mening dat niet in alle gevallen van de op de genoemde site van het OM gebezigde voorbeelden sprake is van hacken? Zo ja, waarom? Zo nee, waarom is er dan wel sprake van hacken?
Op welke strafbare feiten hebben de voorbeelden op de OM site betrekking?

Antwoord 5 en 6
De bedoelde enquête zag op hacken in de zin van computervredebreuk. De in de voorbeelden beschreven handelingen zijn strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht.

Vraag 7, 8 en 9
Deelt u de mening dat hacken enerzijds «computervredebreuk» of andere strafbare feiten en anderzijds verschillende zaken betreffen? Zo ja, waar bestaan de verschillen uit? Zo nee, waarom deelt u de mening niet?
Deelt u de mening dat hackers van belang kunnen zijn bij het melden van kwetsbaarheden in informatiesystemen (bijvoorbeeld door middel van responsible disclosure)? Zo ja, hoe verhoudt zich dat tot het in de context van de criminaliteit plaatsen van hackers? Zo nee, waarom deelt u die mening niet?
Deelt u de mening van de hackersgroepen dat zij door de website van het OM gecriminaliseerd worden en dat de goede naam en reputatie van hackers wordt aangetast? Zo ja, waarom en wat gaat u doen om hier verandering in aan te brengen? Zo nee, waarom niet?

Antwoord 7, 8 en 9
Het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan is strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht. Tegelijk is het samenwerken aan de veiligheid van informatiesystemen en het verstandig en doeltreffend gebruik maken van capaciteiten in de samenleving een belangrijk onderdeel van het kabinetsbeleid op het vlak van cyber security. Het samenwerken via responsible disclosure is daarvan een voorbeeld. In januari 2013 heb ik uw Kamer hierover geïnformeerd en de «leidraad om te komen tot een praktijk van responsible disclosure» toegezonden (Kamerstuk 26 643, nr. 264). Op de website van het Nationaal Cyber Security Centrum is vermeld welke handelingen in ieder geval vermeden dienen te worden. Bovendien worden er verwachtingen en diverse voorbeelden van responsible disclosure benoemd. Zie verder het antwoord op vragen 3 en 4, waarin is aangegeven dat het OM door een welbewust gebruik, onder andere in zijn voorlichting, van de term hacken onnodige criminalisering van hackers voorkomt.