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

158

Vragen van het lid **Gesthuizen** (SP) aan de ministers van Justitie en van Economische Zaken over *de groei en bestrijding van cybercrime* (ingezonden 27 augustus 2010).

Antwoord van minister **Hirsch Ballin** (Justitie en Binnenlandse Zaken en Koninkrijksrelaties), mede namens de minister van Economische Zaken (ontvangen 7 oktober 2010) Zie ook Aanhangsel Handelingen, vergaderjaar 2009–2010, nr. 3367.

Vraag 1
Kent u het bericht over de exponentiële groei van cybercrime in Nederland?[1]

Antwoord 1
Ja.

Vraag 2
Om hoeveel gevallen van cybercrime gaat het jaarlijks? Wordt dit gemeten aan de hand van aangiftes? Zo ja, hoe groot schat u het werkelijke probleem, aangezien niet van alle zaken aangifte gedaan zal worden?

Antwoord 2
Cybercrime is een veelomvattend begrip. Het kan zowel gaan om strafbare gedragingen die niet zonder ICT gepleegd hadden kunnen worden (zoals skimmen, spyware, computervredebreuk, phishing, botnets) als om meer traditionele strafbare gedragingen die met behulp van ICT zijn uitgevoerd (zoals het verspreiden van kinderporno, bedreiging, stalking, handel in illegale goederen, fraude). Door deze diversiteit valt cybercrime niet als apart fenomeen te registreren in de systemen van politie en justitie. Bovendien blijkt uit onderzoek van de Hogeschool Leeuwarden (Verkenning cybercrime in Nederland 2009) dat de aangiftebereidheid bij cybercrime lager ligt dan bij de klassieke vormen van criminaliteit. Om deze redenen kan ik geen indicatie geven van het aantal gevallen van cybercrime.
Het mediabericht waarnaar in vraag 1 wordt verwezen is gebaseerd op het hoofdstuk over high tech crime in het rapport «Overall-beeld aandachtsgebieden» van de Dienst Nationale Recherche. Bij de constatering in dit rapport dat er door de jaren heen sprake is van een exponentiële groei van cybercrime in

[1] http://webwereld.nl/nieuws/66925/cybercrime-in-nederland-groeit-exponentieel.html?utm_source=front_head&utm_medium=website&utm_campaign=ww

ah-tk-20102011-158
ISSN 0921 - 7398
's-Gravenhage 2010

het algemeen en high tech crime in het bijzonder wordt uitdrukkelijk de kanttekening gemaakt dat de constatering wordt gedaan voor zover statistieken voor deelaspecten van cybercrime beschikbaar zijn.

Vraag 3
Hoeveel procent van de aangiftes wordt ook daadwerkelijk opgelost en leidt tot vervolging van de dader(s)? Bent u tevreden over dit resultaat? Zo nee, wat gaat u eraan doen om het oplossingspercentage te verhogen?

Antwoord 3
Zoals toegelicht in mijn antwoord op vraag 2 beschik ik niet over cijfers over het aantal aangiften en het oplossingspercentage. Daarbij moet worden opgemerkt dat in zaken waarin Nederlandse infrastructuur wordt gebruikt voor het plegen van cybercrime of waarin cybercime is gericht tegen Nederlanse burgers en bedrijven, het opsporingsonderzoek kan leiden naar verdachten in het buitenland. De resultaten van een buitenlandse vervolging zijn echter niet inzichtelijk te maken uit de bedrijfsprocessensystemen van politie en OM.
Het opsporen van high tech crime is een van de resultaatgebieden van de Dienst Nationale Recherche. Ik ben tevreden over de voortgang hierbij. Zie daaromtrent verder het antwoord op vraag 5. In het algemeen wijs ik er nog op dat dit kabinet een specifiek intensiveringsprogramma voor de aanpak van cybercrime heeft gestart. Over dit programma bent u in de rapportages «Veiligheid begint bij Voorkomen» geïnformeerd.

Vraag 4
Wat is uw reactie op de bevindingen in het rapport van het Korps Landelijke Politiediensten (KLPD)?[2] Bent u bereid dit rapport, voorzien van uw reactie, aan te bieden aan de Kamer?

Antwoord 4
Het bedoelde rapport is openbaar en beschikbaar via de website van het KLPD. Niet iedere analyse of rapportage vanuit de politie wordt door mij – voorzien van een beleidsreactie – aan de Tweede Kamer aangeboden. Voor zover relevant wordt ook de informatie uit deze rapportage meegenomen in de beleidsvorming waarover u steeds op geëigende wijze wordt geïnformeerd.

Vraag 5
Waar zitten volgens u de knelpunten voor een effectief optreden van de politie? Hoe gaat u deze knelpunten aanpakken?

Antwoord 5
Ik ben tevreden over de voortgang die de afgelopen jaren is gemaakt bij de aanpak en opsporing van cybercrime en high tech crime. Meer partijen werken samen, het kennisniveau is gestegen, en er zijn successen geboekt. Essentieel voor dit aandachtsgebied is dat er voldoende gelegenheid is voor kennisopbouw, productontwikkeling en innovatie, zodat de opsporing gelijke tred kan houden met de steeds geavanceerder wordende dreiging. Dit wordt onder andere bevorderd doordat de Dienst Nationale Recherche zich focust op de «high tech» of bijzondere vormen van cybercrime. Tegelijkertijd is voor het verkrijgen van een goed beeld van de aard en omvang van cybercrime, noodzakelijk dat slachtoffers daarvan consequent aangifte doen. Het intensiveringsprogramma «aanpak cybercrime» is mede hierop gericht. Een ander kenmerkend knelpunt voor cybercrime is het internationale karakter ervan, waardoor een goede grensoverschrijdende samenwerking en kennisuitwisseling tussen de opsporingsdiensten een absolute vereiste is. Voor de activiteiten die Nederland op internationaal vlak onderneemt verwijs ik naar het antwoord op vraag 9.

Vraag 6
Welke mazen zitten er in de wet die effectieve aanpak van cybercrime in de weg staan? Hoe gaat u ervoor zorgen dat deze problemen op korte termijn opgelost worden?

[2] Overall-beeld Aandachtsgebieden Nationale Recherche (KLPD)

Antwoord 6
Het wetgevend kader op dit terrein is voortdurend in ontwikkeling. Ik verwijs u bijvoorbeeld naar de openbare internetconsultatie over het wetsvoorstel Computercriminaliteit III . Deze consultatie zal helpen om een helder beeld te krijgen van de actuele knelpunten in wet- en regelgeving. Verder merk ik op dat de bestrijding van cybercrime gezien de internationale aard ervan vraagt om internationale regels en afspraken. Daarvan zijn er al de nodige gemaakt, met name in het cybercrimeverdrag van de Raad van Europa. Ook het internationaal regelgevend kader is voortdurend in ontwikkeling. Helaas is dit niet iets dat op korte termijn uitputtend en sluitend geregeld kan worden.

Vraag 7
Wat is uw reactie op het feit dat vooral Nederland een belangrijke bron is van cyberaanvallen? Wat betekent dit voor de benodigde opsporingscapaciteit? Is deze capaciteit volgens u voldoende op peil? Zo nee, wat gaat u hieraan doen?

Antwoord 7
Dat Nederland een belangrijke bron is van cyberaanvallen hangt vermoedelijk samen met de omstandigheid dat Nederland wereldwijd een van de grootste internetknooppunten is, een zeer goede technische infrastructuur heeft, en dat er veel hosting- en servercapaciteit in Nederland is. Dit trekt criminelen aan, hetgeen vanzelfsprekend extra druk op de opsporing legt. De herkomst van de cyberaanvallen zegt overigens niets over de locatie van de cybercriminelen zelf. Deze maken meestal gebruik van weer andere servers in het buitenland, om zodoende hun identiteit te verhullen. De vraag of de ingezette opsporingscapaciteit voor cybercrime voldoende is, is niet met een eenvoudig ja of nee te beantwoorden. Politie en justitie zullen nooit alle werkzaamheden die op hen afkomen volledig kunnen oppakken. Er moet altijd een afweging tussen verschillende opsporingsbelangen worden gemaakt.

Vraag 8
Wat is uw reactie op de uitspraken van een oud-politierechercheur en informatiebeveiligingsspecialist dat cybercrime vrijwel onvervolgbaar is, en dat het kennisniveau bij de politie wat betreft cybercrime laag is?[3]

Antwoord 8
Deze uitspraken onderschrijf ik niet. Het klopt weliswaar dat mede vanwege het internationale karakter van cybercrime het vervolgen ervan lastig en een vervolging in Nederland soms niet mogelijk is, maar inmiddels is ook gebleken dat zelfs uiterst complexe zaken in internationaal verband met succes aangepakt kunnen worden. Wat betreft het kennisniveau bij politie is het van belang in ogenschouw te nemen dat de aanpak van cybercriminaliteit nog in ontwikkeling is. De aanpak daarvan vereist andere, aanvullende, kennis en vaardigheden bij politie en justitie. Dit is wereldwijd het geval. In Nederland is in 2007 het eerder genoemde intensiveringsprogramma opgezet om onder andere in het verspreiden en opbouwen van kennis en vaardigheden te investeren. Voor de aanpak van bijvoorbeeld phishing en botnets zijn zogenaamde proeftuinen ingericht. Het kennisniveau bij gespecialiseerde afdelingen zoals het Team High Tech 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 high tech crime.

Vraag 9
Bent u bereid op internationaal vlak te pleiten voor het snel op elkaar aan laten sluiten van wetgeving, zodat criminelen makkelijker aangepakt kunnen worden? Bent u bereid in overleg te treden met uw internationale collega's en Eurocommissaris Kroes, om zo tot een internationaal actieplan te komen?

Antwoord 9
Ja. Nederland heeft het cybercrimeverdrag van de Raad van Europa ondertekend en geratificeerd. Binnen het overleg van verdragsluitende landen op grond van artikel 46 van dit verdrag, is Nederland zeer actief. Binnen de Europese Unie heeft Nederland met concrete voorstellen bijgedragen aan de

[3] http://computerworld.nl/article/1290 «Nederland topland voor cybercrime»

tekst van de cybercrimeparagraaf in het zogenoemde «Stockholmprogramma». De uitvoering van de daarin opgenomen akties betreft mede de portefeuille van Eurocommissaris Kroes, maar ook die van haar collega's Malmström en Reding.

Vraag 10
Wat is uw reactie op de constatering dat vooral het MKB slachtoffer is van cybercrime? Hoe kunnen zij beter beschermd worden en bent u bereid passende maatregelen te nemen?

Antwoord 10
Ik vind deze constatering uiteraard zorgelijk. Mijn collega van Economische Zaken en ik blijven ons inspannen om de bewustwording van de risico's bij bedrijven te vergroten. Het hebben van actuele kennis over innovatieve technologieën en bewustwording over internetveiligheid is essentieel voor het kunnen nemen van passende preventieve maatregelen. Daartoe is in het kader van het Actieplan Veilig Ondernemen in samenwerking met MKB-Nederland een campagne gevoerd waarbij concrete tips zijn aangereikt om systemen te beveiligen. In oktober is in het kader van het programma Digivaardig & Digibewust een wachtwoordencampagne gericht op het MKB voorzien. Ook in dit verband is het van belang dat consequent aangifte wordt gedaan van gevallen van cybercrime.

Vraag 11
Kent u het bericht over fraude op internet?[4]

Antwoord 11
Ja.

Vraag 12
Wat is uw reactie op het feit dat ook hier blijkt dat met name het MKB slachtoffer is van deze praktijken?

Antwoord 12
Ik kan niet bevestigen dat het met name de kleine internetwinkels zijn die slachtoffer worden van fraude met PayPal-accounts. Vermoedelijk treft dit de grote bedrijven even zeer, maar zit het verschil vooral in de impact van de fraude op de bedrijfsvoering van de internetwinkels. Van PayPal heb ik vernomen dat het aantal fraudegevallen slechts 0,2 procent van het totaal aantal transacties bedraagt. Desalniettemin blijft aandacht hiervoor vereist. Thans wordt een proeftuin landelijk meldpunt internetoplichting ingericht. Vanaf 7 oktober aanstaande zal online melding kunnen worden gemaakt wanneer men slachtoffer is geworden van internetoplichting. Op basis van deze meldingen zal een lijst worden samengesteld van de grootste internetoplichters, zodat de opsporing in dit domein meer gericht kan worden ingezet.

Vraag 13
Wat gaat u doen om particulieren en bedrijven beter te beschermen tegen dergelijke praktijken?

Antwoord 13
Naast wettelijke bepalingen voor fraude en oplichting waar zowel particulieren als bedrijven zich op kunnen beroepen, hebben zij ook een eigen verantwoordelijkheid. Particulieren moeten zich bewust zijn van de kenmerken van de verschillende online transactiediensten. Bedrijven hebben een zorgplicht richting hun klanten voor de veiligheid en betrouwbaarheid van de door hen aangeboden online transactiediensten. Als de ondernemer of de consument het niet veilig genoeg vindt om de betaling via een online transactiedienst te laten verlopen, dan kan hij er in het ultieme geval voor kiezen om met die partij geen zaken te doen. Voorlichting speelt hierbij een belangrijke rol. Met de Postbus 51 campagne Veilig Internetten is de afgelopen twee jaar aandacht gevraagd voor de eigen verantwoordelijkheid

[4] http://www.metronieuws.nl/algemeen/fraude-op-internet-webshopje-de-klos/SrZjhx!VqMmzvCZZSw/

en de mogelijkheden die men zelf heeft om veilig gebruik te maken van webdiensten. In de campagne van afgelopen zomer is daarbij expliciet aandacht besteed aan veilige online transacties. Dat het belang ervan breed leeft blijkt ook uit de recent aangekondigde campagnes en acties rond ondermeer veilig bankieren en betalen van bijvoorbeeld de Consumentenbond en de Nederlandse Vereniging van Banken.

Vraag 14
Herinnert u zich uw antwoorden op schriftelijke Kamervragen van de SP fractie met betrekking tot internetoplichting nog?[5]

Antwoord 14
Ja.

Vraag 15
Deelt u de mening dat kennisversterking bij politie en aangiftebereidheid van slachtoffers slechts een deel van de oplossing is, en dat de politie nog onvoldoende mogelijkheden heeft om effectief op te kunnen treden tegen deze vormen van fraude? Zo ja, hoe gaat u ervoor zorgen dat dit op peil wordt gebracht? Zo nee, waarom niet?

Antwoord 15
Het is juist dat de bestrijding van cybercrime een samenspel van maatregelen behoeft. Daarvan maken kennisversterking bij de politie en aangiftebereidheid van slachtoffers een belangrijk deel uit. Even zo belangrijk is het vergroten van de opsporingscapaciteit en het voorhanden zijn van een adequaat juridisch instrumentarium om effectief te kunnen optreden. Ik deel dan ook niet de zeer algemene conclusie dat de politie onvoldoende mogelijkheden heeft om op te treden tegen internetoplichting. Ik verwijs u verder naar de antwoorden die ik heb gegeven op de schriftelijke vragen waarnaar u in vraag 14 verwijst, en naar de antwoord op uw vragen 3, 5, 6, 7, 8 en 9.

[5] Aanhangsel Handelingen, vergaderjaar 2009–2010, nr. 2511.