Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

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

2703

Vragen van het lid **Recourt** (PvdA) aan de Minister van Veiligheid en Justitie over *het bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost* (ingezonden 13 juni 2014).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 14 augustus 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 2457.

Vraag 1
Kent u het bericht «Cybercrime kost Nederland 8,8 miljard euro per jaar», het bericht «Nadelen internet worden te groot» en het bericht «Bedrijven komen in actie tegen digitaal onheil»?[1] [2] [3] Heeft u voorts kennisgenomen van het rapport «Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II»?[4]

Antwoord 1
Ja.

Vraag 2 en 3
Acht u de conclusie uit het hierboven genoemde rapport juist dat cybercrime in Nederland jaarlijks een verliest oplevert van 1,5% van het Bruto Nationaal Product (BNP)? Zo ja, waarom? Zo nee, waarom niet en over welke cijfers beschikt u?
Weet u waarom het verlies ten gevolge van cybercrime uitgedrukt in een percentage van het BNP in Nederland relatief hoog is? Zo ja, wat zijn de oorzaken van dit hoge percentage? Zo nee, waarom weet u dit niet en acht u het alsnog vergaren van dergelijke kennis relevant voor een gerichte aanpak van cybercrime in Nederland?

[1] «Cybercrime kost Nederland 8,8 miljard euro per jaar, NU.nl, 9 juni 2014 (http://www.nu.nl/internet/3795902/cybercrime-kost-nederland-88-miljard-euro-per-jaar.html)
[2] «Nadelen internet worden te groot», Het Financieele Dagblad, 10 juni 2014
[3] «Bedrijven komen in actie tegen digitaal onheil», Het Financieele Dagblad, 10 juni 2014
[4] «Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II», Center for Strategic and International Studies/McAfee, June 2014 (http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf)

ah-tk-20132014-2703
ISSN 0921 - 7398
's-Gravenhage 2014

Antwoord 2 en 3
De economische schade als gevolg van cybercrime is lastig te becijferen. Ik kan de gegevens daarom niet bevestigen. Het rapport meldt dat vooral de verschillen in de grondigheid van de registratie de variaties tussen landen verklaren. Daarnaast behoort de Nederlandse digitale infrastructuur tot de beste van de wereld, maken Nederlanders gemiddeld veel gebruik van digitale diensten ten opzichte van andere landen en gebruikt veel internationaal internetverkeer de Nederlandse infrastructuur. Ook dat kunnen redenen zijn de gevolgen van cybercrime in Nederland naar verhouding hoog in te schatten. Het rapport bevat bovendien een ruime omschrijving van cybercrime.

Vraag 4
Deelt u de mening dat cybercrime niet alleen het belang van het Nederlandse bedrijfsleven raakt, maar ook het publieke belang van onze nationale economie? Zo ja, betekent dit dat meer dan nu het geval de overheid een grotere rol op zich zou moeten nemen in de bestrijding van cybercrime? Zo nee, waarom niet?

Antwoord 4
Ja. De mogelijkheden van het internet zijn voor Nederlandse burgers, bedrijven en de overheid van groot belang. Cybercrime heeft niet alleen directe schade voor de betrokkenen tot gevolg, maar leidt ook tot schade voor de samenleving en de economie als geheel. Zo vormen digitale spionage en sabotage een bedreiging voor de nationale veiligheid en economie. Cybercrime ondergraaft het vertrouwen in het internet en digitale dienstverlening in het algemeen. Daarom besteedt de Nederlandse regering veel aandacht aan cyber security. Op 28 oktober 2013 heb ik namens het kabinet de tweede Nationale Cyber Security Strategie (NCSS) aan uw Kamer gestuurd. Daarin heb ik gemeld dat de overheid een meer nadrukkelijke rol zal gaan spelen in het cyberdomein, enerzijds door zelf te investeren in de veiligheid van de eigen netwerken en diensten en anderzijds door partijen bij elkaar te brengen en beschermend op te treden als bijvoorbeeld de veiligheid van bedrijven of burgers wordt bedreigd. Verder zal de overheid waar nodig kader- en normstellend optreden.
De politie en het OM hebben de afgelopen jaren veel aandacht besteed aan het opbouwen van de capaciteit voor de opsporing en vervolging van cybercrime. De politie heeft met het *Team High Tech Crime* een kundige capaciteit voor de opsporing van cybercrime opgebouwd en werkt nu aan de verdere uitbreiding en professionalisering daarvan. Ook is de opbouw van digitale expertise in de regionale eenheden van de politie voorzien. Bij het OM zijn speciale officieren belast met de vervolging van cybercrime en zij hebben daarvoor een aanvullende opleiding genoten.
De AIVD heeft in het kader van de nationale veiligheid de afgelopen jaren het onderzoek naar digitale aanvallen gericht op spionage en sabotage geïntensiveerd. Inzicht in digitale aanvallen wordt gedeeld met getroffen partijen en ingezet ten behoeve van een betere detectie en preventie. De AIVD informeert de overheid en samenleving over digitale dreigingen en geeft advies over informatiebeveiliging.
Tenslotte heb ik in het voorjaar het wetsvoorstel Computercriminaliteit III voor advies aan de Raad van State gezonden. Dit wetsvoorstel beoogt onder meer de bevoegdheden van de politie voor de bestrijding van cybercrime en gedigitaliseerde criminaliteit te versterken.

Vraag 5
Hoe is de regie over de verschillende overheidsdiensten en de samenwerking tussen de Ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Veiligheid en Justitie geregeld als het om digitale beveiliging en de afstemming met het bedrijfsleven ten aanzien van cybercrime gaat?

Antwoord 5
De ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, en Veiligheid en Justitie hebben een hechte samenwerking op het gebied van cyber security. Er zijn op diverse niveaus periodieke overleggen en de activiteiten van de ministeries worden, vanuit de eigen verantwoorde-

lijkheid van elke organisatie, op elkaar afgestemd. In mijn rol als coördinerend bewindspersoon voor cyber security ben ik verantwoordelijk voor die samenwerking. Daarnaast zoeken de betrokken ministeries actief de samenwerking met private partners.
De totstandkoming van de tweede NCSS is een voorbeeld van de samenwerking tussen de overheid en private partners. Private partners waren vertegenwoordigd in het redactieteam van de strategie. Daarnaast zijn ten behoeve van de strategie twee brede bijeenkomsten georganiseerd om zo veel mogelijk inhoudelijke bijdragen van private partijen te betrekken.

Vraag 6
Wat is uw mening over het feit dat de overheid geen deelnemer is aan het de Nationale anti-DDoS Wasstraat (project NaWas) dat DDoS-aanvallen moet weren?

Antwoord 6
Het Project Nationale anti-DDoS Wasstraat, ofwel project Nawas, is een privaat en gezamenlijk initiatief van diverse providers om een gezamenlijke voorziening in te richten om een overvloed aan verkeer, zoals plaatsvindt bij DDoS-aanvallen, te schonen. Het Nationaal Cyber Security Centrum (NCSC) is vanuit haar rol als netwerkpartner en stimulator van ontwikkelingen in het cyber securityveld voorstander van het ontwikkelen van business cases door private partijen die bijdragen aan digitale veiligheid, en volgt deze met aandacht. Het is uiteindelijk aan klanten, publiek en privaat, om de afweging te maken of deze dienst wordt afgenomen. Het NCSC ondersteunt daar waar mogelijk en noodzakelijk initiatieven op het gebied van digitale veiligheid.

Vraag 7
Deelt u de mening dat naar het voorbeeld van het stelsel bewaken en beveiligen van personen en gebouwen er ook een stelsel bewaken en beveiligen zou moeten zijn waarin duidelijk wordt vastgelegd in hoeverre bedrijven zelf verantwoordelijk zijn voor hun beveiliging tegen cybercrime en wanneer daar een taak van de overheid ligt? Zo ja, is een dergelijk stelsel er al, door wie wordt dat uitgevoerd en op basis van welke concrete regelgeving gebeurt dat? Zo nee, acht u een dergelijk stelsel wenselijk en hoe en op welke termijn gaat u dit vormgeven?

Antwoord 7
Ten aanzien van verantwoordelijkheden op het terrein van cybersecurity geldt, analoog aan het fysieke domein, dat bedrijven primair een eigen verantwoordelijkheid kennen op het gebied van informatiebeveiliging. De afgelopen jaren is ingezet op het borgen van sectorale verantwoordelijkheden en het realiseren van een sluitend stelsel van sectorale regelgeving en interventiemogelijkheden in verband met cybersecurity. Hierover heb ik uw Kamer geïnformeerd in mijn brieven van 23 december 2011 en 6 juli 2012.[5] Verder verwijs ik kortheidshalve naar de tweede NCSS.

Vraag 8
Herkent u het beeld dat bedrijven die slachtoffer zijn geworden van cybercrime terughoudend zijn in het doen van aangifte, bijvoorbeeld vanwege de vrees van reputatieschade? Zo ja, wat gaat u doen om deze aangiftebereidheid te vergroten en in hoeverre is het doen van anonieme aangifte een mogelijkheid om deze aangiftebereidheid te vergroten?

Antwoord 8
De vrees voor reputatieschade kan in bepaalde gevallen voor bedrijven een overweging zijn om geen ruchtbaarheid te geven aan een cyberaanval. In nauwe samenwerking tussen publieke en private partijen is binnen de bewustwordingscampagne «Stopcybercrime.nu» van MKB-Nederland een hulpknop ontwikkeld waar informatie over typen cybercriminaliteit op één punt vindbaar is en waar bedrijven die slachtoffer zijn of denken te zijn geworden direct een handelingsperspectief wordt geboden. Daarbij wordt ook de mogelijkheid van het doen van een melding of aangifte toegelicht. Verder

[5] Kamerstukken II, cergaderjaar 2011–2012, 26 643, nrs. 220 en 245.

is het versterken van het intake- en registratieproces van aangiften cybercrime een actiepunt uit de tweede NCSS.
Het tijdens een strafrechtelijk onderzoek en strafproces (tot op zekere hoogte) afschermen van de identiteit van een aangever is in beginsel alleen mogelijk als er sprake is van een uitzonderlijke, bedreigende situatie jegens de aangever.
Naast het inzetten van het strafrecht maken andere interventiemethoden deel uit van een integrale aanpak van cybercrime. Daarbij werken publieke ketenpartners en private partijen samen. Bij het NCSC kunnen bijvoorbeeld cyberincidenten vertrouwelijk worden gemeld, zodat andere organisaties kunnen worden geïnformeerd en (verdere) schade kan worden voorkomen. Het NCSC kan organisaties bovendien begeleiden en adviseren in de afhandeling van een cyberincident.

Vraag 9 en 10
In hoeverre is de huidige wijze van strafrechtelijke vervolging nog geschikt om cybercriminelen aan te pakken die misdrijven over de hele wereld plegen?
In hoeverre levert het gebrek aan een uitleververdrag met sommige landen cybercriminelen in die landen een vrijhaven op voor hun activiteiten? Acht u het wenselijk om in onderhandelingen over handelsverdragen met die landen ook aandacht te schenken aan de mogelijkheid van (internationale) vervolging en van uitlevering van cybercriminelen? Zo ja, op welke wijze wilt u dat doen? Zo nee, waarom niet?

Antwoord 9 en 10
Cybercrime is bij uitstek een grensoverschrijdend probleem. Door internationale samenwerking bij de opsporing van cybercrime zijn inmiddels stevige successen geboekt. De internationale opsporing en vervolging is niet (enkel) afhankelijk van het bestaan van bilaterale rechtshulp- of uitleveringsverdragen. Het multilaterale Cybercrimeverdrag uit 2001, gesloten in het kader van de Raad van Europa, bevat afspraken voor het strafbaar stellen van bepaalde vormen van cybercrime en voor wederzijdse hulp bij de opsporing en de vervolging. Inmiddels zijn 42 landen aangesloten bij het verdrag. Nederland ondersteunt de Raad van Europa bij het onder de aandacht brengen van het cybercrimeverdrag bij landen die nog niet zijn aangesloten. Overigens zijn er ook niet-aangesloten landen waarvan de nationale wetgeving wel in lijn is met het Cybercrimeverdrag. Als internationale samenwerking vanwege georganiseerde cybercrime aan de orde is, kan daarnaast het VN-verdrag ter bestrijding van grensoverschrijdende georganiseerde criminaliteit (UNTOC-verdrag) dienen als rechtsbasis voor rechtshulpverlening of uitlevering. Bij dit verdrag zijn 176 landen aangesloten. Vanwege deze verdragen is er geen aanleiding om vervolging en uitlevering van cybercriminelen te betrekken bij onderhandelingen over handelsverdragen. Dit onderwerp sluit bovendien niet aan op het bereik en de inhoud van onderhandelingen over handelsverdragen.
Om de internationale samenwerking bij de opsporing en vervolging van cybercrime te versterken wil Nederland een voortrekkersrol vervullen om te komen tot een verdere harmonisering van de wetgeving op dit gebied. Overigens zal het bereiken van internationale consensus hierover nog de nodige tijd vergen. Verder ondersteunt Nederland in het kader van het Cybercrimeverdrag projecten voor capaciteitsopbouw in landen waar dat nodig is. Inzetbare, kundige capaciteit is immers een basisvoorwaarde voor het daadwerkelijk opsporen en vervolgen van (grensoverschrijdende) cybercrime. De doelgroep hiervan zijn de landen die zich willen aansluiten of onlangs hebben aangesloten bij het cybercrimeverdrag.