Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

34 034 Implementatie van de richtlijn 2013/40/EU van het Europees parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8)

Nr. 4

VERSLAG

Vastgesteld 25 november 2014

De vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

Inhoudsopgave

1. Inleiding

De leden van de VVD-fractie hebben kennisgenomen van het wetsvoorstel ter implementatie van richtlijn 2013/40/EU van het Europees parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van het Kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8) hierna: het wetsvoorstel. Het doet deze leden deugd dat de strafbaarstellingen van computercriminaliteit worden aangescherpt en de strafverzwarende omstandigheden worden toegevoegd. De impact van cybercrime op de samenleving neemt nog steeds toe evenals de belangen van burgers, bedrijven en overheden bij een veilige en betrouwbare digitale en vitale infrastructuur. Het is daarbij van groot belang dat een duidelijk signaal wordt afgegeven en een stevige aanpak mogelijk wordt gemaakt. Daarbij is het noodzakelijk en onvermijdelijk dat wordt aangesloten bij de internationale ontwikkelingen en bij de bestaande wetgeving.

De leden van de VVD-fractie hechten grote waarde aan de internationale publiek-private samenwerking ter preventie en bestrijding van cybercrime. Daarbij merken deze leden op dat in de memorie van toelichting wordt

kst-34034-4
ISSN 0921 - 7371
's-Gravenhage 2014

gesproken over voorschriften om informatie uit te wisselen en een 24/7 netwerk van contacten ten behoeve van cybercrime. Gezien de vele betrokken partners willen voornoemde leden graag weten welke organisaties vanuit Nederland hierbij betrokken zijn en wat de onderlinge verhoudingen zijn. In het bijzonder vragen zij of het departement met het Nationaal Cyber Security Centrum (NCSC) nog steeds de regie heeft en eindverantwoordelijk is. Hoe verloopt de samenwerking met de private sector en wat is in Nederland de rol van de onlangs in Den Haag gevestigde cybereenheid van de NAVO?

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van voornoemd wetsvoorstel. Deze leden zijn zich bewust van de grote gevolgen van een aanval op computersystemen die vitale onderdelen van de economie sturen en de maatschappelijke ontwrichting die dit tot gevolg kan hebben. Hiertoe is strenge, doch heldere wetgeving nodig. Niet alleen de strafrechtelijke aanpak is belangrijk teneinde cybercriminaliteit aan te pakken, ook het voorkomen van cybercriminaliteit moet voldoende aandacht krijgen. Zij pleiten daarom ook voor brede wetgeving ten aanzien van het dataverkeer, juist om breed in te kunnen zetten op het voorkomen en het bestrijden van cybercriminaliteit, het beschermen van vitale datanetwerken en aan de andere kant de bescherming van de persoonsgegevens.

De leden van de PvdA-fractie merken op dat het Openbaar Ministerie (OM) in haar advies pleit voor één titel in het Wetboek van Strafrecht (Sr) waarin alle strafbepalingen ten aanzien van cybercriminaliteit worden opgenomen. De regering wil dit voorstel niet ondersteunen maar nader afwegen. Komt de regering hier nog op terug?
Aanpak van cybercriminaliteit kan alleen succesvol zijn als alle EU-lidstaten de EU-richtlijnen en EU-verdragen onderschrijven. Deelt de regering die mening? Zo nee, waarom niet? Welke EU-lidstaten hebben het Kaderbesluit 2005/222/JBZ ondertekend? Welke lidstaten niet en wat is daarvan de reden? Zijn die lidstaten nu wel aangesloten bij deze EU-richtlijn over de aanpak van cybercriminaliteit? Mondiaal moet nog veel werk worden verzet. Een klein aantal landen heeft het verdrag van Roemenië ondertekend (Goedkeuring van het op 28 januari 2003 te Straatsburg tot stand gekomen aanvullend Protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, betreffende de strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen (Trb. 2003, 60 en Trb. 2005, Kamerstuk 31 838-R1874). Een groot deel van deze landen ligt in Europa. Slechts een beperkt aantal landen buiten Europa is aangesloten bij dit verdrag en dus bij de bestrijding van cybercriminaliteit. Welk signaal gaat hiervan uit? Hoe kan cybercriminaliteit effectief bestreden worden als niet alle landen hiertoe samenwerken? Is er een groot verschil van mening hoe omgegaan moet worden met data in het algemeen tussen de bij het verdrag aangesloten landen en de landen die niet zijn aangesloten?

Begrijpen de leden van de PvdA-fractie het goed dat één van de taken van het Team High Tech Crime (THTC) is het verzamelen en doorgeven van gegevens over de in de EU-richtlijn bedoelde strafbare feiten. Zo nee, wie verzamelt en wie verwerkt deze gegevens dan? Zo ja, om welke specifieke gegevens gaat het? Hoe vaak worden deze gegevens verzameld en hoe vaak worden deze gegevens doorgegeven en aan wie? Kennen andere EU-lidstaten eenzelfde frequentie ten aanzien van het doorgeven van informatie in het kader van bestrijding cybercriminaliteit als Nederland?

De leden van de SP-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij begrijpen dat de discussie over een afzonderlijke titel in het Wetboek van Strafrecht niet past binnen dit wetsvoorstel, maar hebben hier toch een paar vragen over. Ervaren politie en justitie knelpunten doordat de verschillende strafbare feiten verspreid over het Wetboek van Strafrecht staan? Acht de regering het wenselijk met een afzonderlijke titel te komen? In hoeverre is de regering van plan niet alleen het Wetboek van Strafvordering te moderniseren, maar ook het Wetboek van Strafrecht?

De leden van de PVV-fractie hebben kennisgenomen van bovengenoemd wetsvoorstel en hebben hierbij nog enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van onderhavig wetsvoorstel. Zij hebben daarover nog enkele vragen. Kan de regering cijfermatig de stellingname staven dat zij de toenemende risico's van cybercriminaliteit krachtig wil aanpakken. Doet het voornemen in 2015, 25 complexe onderzoeken en 175 reguliere onderzoeken uit te voeren naar cybercrime, recht aan de omvang van de veronderstelde problematiek in de begrotingsstaten van het Ministerie van Veiligheid & Justitie voor het jaar 2015. (Kamerstuk 34 000 VI, prestatie-indicatoren Veiligheidsagenda Blz. 22) Kan de regering een overzicht geven van alle (bekende) grootschalige cyberaanvallen in Nederland die zich de afgelopen twee jaar hebben voorgedaan, zowel in het bedrijfsleven als bij de overheidsinstanties? Wat verstaat de regering onder grootschalige cyberaanvallen? Wat is de jaarlijks geschatte maatschappelijke schade als gevolg van cybercrime? Hoeveel strafrechtelijke opsporingsonderzoeken, zowel complexe als reguliere, zijn de afgelopen twee jaar opgestart naar mogelijke overtreding van de artikelen 138ab, 138b, 139ba t/m 139e, 161sexies en 161septies, 326c, 350a, 350b, 351 en 351bis Sr? Kan de regering een overzicht per artikel geven, uitgesplitst naar onderzoeken ambtshalve opgestart en na aangifte? Deze leden vernemen in dit overzicht graag ook de uitkomsten van de strafrechtelijke vervolging en van de berechting.

De aan het woord zijnde leden vragen voorts of de regering kan aangeven hoeveel fte de afgelopen twee jaar beschikbaar waren en de komende twee jaar zijn voor het THTC van de Dienst Nationale Recherche van de Landelijke Eenheid van de nationale politie, alsmede eenzelfde overzicht van het aantal officieren van justitie dat zich specifiek richt op de vervolging van strafrechtelijke cybercrimedelicten.

Voornoemde leden vragen of de regering de inschatting van de beheerder van DigiD, Logius, kan bevestigen dat ongeveer 1000 keer per jaar een DigiD geblokkeerd wordt omdat er vermoedens zijn van misbruik (zie uitzendingen «Opgelicht», 28 oktober en 11 november 2014, http://www.opgelicht.nl/dossiers/detail/7727/). Zij vragen of de regering kan aangeven of in de afgelopen twee jaar het DigiD-systeem voorwerp is geweest van een of meer cyberaanvallen en of het klopt dat meerdere gemeenten kwetsbaar zijn geweest in 2014 voor DigiD-misbruik. Kan de regering meer inzicht geven in het beveiligingsprobleem in de systemen van de betreffende gemeenten? Welke gemeenten betreft het en welke maatregelen zijn inmiddels genomen teneinde het probleem op te lossen?

De leden van de CDA-fractie vragen de regering of het klopt dat in het conceptwetsvoorstel computercriminaliteit III, waarover de Afdeling Advisering van de Raad van State advies heeft uitgebracht, geen afzonderlijke titel in het Wetboek van Strafrecht is opgenomen ten aanzien van cybercrimedelicten. Deze leden vernemen graag in hoeverre uit dit conceptwetsvoorstel blijkt dat er nog een nadere afweging moet

plaatsvinden omtrent het wel of niet opnemen van een afzonderlijke titel. Kan de regering alle voor-en nadelen hiervan opsommen, aangezien zij in reactie op het advies van het OM op onderhavig wetsvoorstel enkel aangeeft dat de huidige plaatsing van de artikelen aansluit bij de gepleegde gedragingen.

2. Hoofdlijnen wetsvoorstel

De leden van de VVD-fractie lezen in de memorie van toelichting dat wordt aanbevolen bij een daarvoor geschikte gelegenheid een titel in het Wetboek van Strafrecht te creëren met betrekking tot cybercriminaliteit. De regering geeft in de memorie van toelichting aandacht hieraan. Deze leden vragen of bij de komende herijking van het Wetboek van Strafvordering hier ook rekening mee wordt gehouden en zo ja op welke wijze hieraan invulling zal worden gegeven?

De leden van de CDA-fractie zijn het eens met de keuze van de regering de voorgestelde artikelen 350c en 350d Sr alsnog te koppelen aan het strafvorderlijk middel van de voorlopige hechtenis. Deze leden zijn benieuwd of de regering per abuis de voorgestelde artikelen 350c en 350d Sr niet onder de werking van artikel 67 van het Wetboek van Strafvordering (Sv) heeft gebracht of dat daar een bewuste keuze aan ten grondslag heeft gelegen.

De leden van de PVV-fractie lezen in de memorie van toelichting dat bestaande wettelijke bepalingen een ruimere bescherming bieden dan de voorgestelde EU-richtlijn. Ook lezen zij dat Nederland, op artikel 9 van de EU-richtlijn na, al voldoet aan hetgeen waartoe de EU-richtlijn verplicht. Deze leden vragen wat de meerwaarde is van deze implementatiewetgeving voor Nederland.
Kan de regering de meerwaarde van deze implementatiewet voor Nederland met ten minste vijf argumenten onderbouwen? Welke lacunes zijn er op dit moment in de Nederlandse wetgeving op het gebied van aanvallen op informatiesystemen waaruit zou moeten blijken dat de implementatiewet noodzakelijk is?
Wat zijn de gevolgen voor de Nederlandse burger indien deze EU-richtlijn niet geïmplementeerd zal worden? Hoeveel Nederlanders zullen hier schade of nadeel van ondervinden? Is naar deze nadelige gevolgen onderzoek gedaan?
Heeft de regering bij dit wetsvoorstel een subsidiariteits- en proportionaliteitstoets uitgevoerd? Zo nee, waarom niet? Hoe gaat de regering ervoor zorgen dat de verschillende vormen van computercriminaliteit daadwerkelijk beter opgespoord en harder bestraft zullen gaan worden?

3. Inhoud richtlijn en wijze van implementatie

De leden van de VVD-fractie merken het navolgende op over de werking van artikel 7 van de EU-richtlijn die onder andere ziet op het tegengaan van het vervaardigen van kwaadaardige software. Deze leden vragen of en hoe het rechtmatig vervaardigen van programma's, die zowel goedschiks als kwaadschiks kunnen worden gebruikt en voor zover deze programma's nodig zijn ten behoeve van goedschikse inzet, door de veiligheidsdiensten en de politie mogelijk blijft. Het lijkt deze leden niet wenselijk als een oneerlijk speelveld ontstaat voor Europese bedrijven en de Nederlandse veiligheidsdiensten zich bij voorbaat moeten richten op aanbieders buiten de EU. Daarnaast lijkt het de aan het woord zijnde leden onwenselijk dat de Nederlandse veiligheidsdiensten hun schaarse capaciteit moeten aanwenden teneinde zelf dergelijke programma's te vervaardigen. Graag ontvangen zij een reactie van de regering op de (on)mogelijkheden van een rechtmatige productie en het toezicht daarop.

De leden van de SP-fractie willen weten of de spionagesoftware van de politie zoals Finfisher onder de strafbaarstelling valt van artikel 7, onder a, van de EU-richtlijn c.q. artikel 6, eerste lid, van het Cybercrimeverdrag, aangezien het een computerprogramma betreft dat geschikt gemaakt is voor bijvoorbeeld doorzoeking van gegevensdragers?[1] Zo nee, waarom niet? Graag ontvangen deze leden daarop een uitgebreide toelichting van de regering. Kan worden toegelicht wat in de artikelen 7 en 9 van de EU-richtlijn wordt bedoeld met het «hoofdzakelijk» geschikt maken of ontwerpen van computerprogramma's voor het plegen van de daarbij genoemde strafbare feiten? Wat is hoofdzakelijk en waar ligt de grens? Kan een softwareprogramma er dan ook een beetje geschikt voor zijn? Deze leden zijn benieuwd waarom is gekozen voor een maximumstraf van twee jaar. Waarom heeft Nederland niet zelf voor die termijn gekozen bij de totstandkoming van nationale wetgeving?

De leden van de SP-fractie constateren dat een strafverzwarende omstandigheid kan zijn dat het feit ernstige schade tot gevolg heeft. Wat wordt er verstaan onder deze ernstige schade? Wanneer is schade derhalve ernstig genoeg?
De EU-richtlijn verplicht verder dat er statistische gegevens worden geregistreerd over de in de artikelen 3 tot en met 7 van de EU-richtlijn bedoelde strafbare feiten. Wat is hier het doel? Worden ook gegevens geregistreerd over het aantal personen dat is vervolgd maar wel is vrijgesproken of is veroordeling noodzakelijk? De leden van de SP-fractie zijn tot slot benieuwd naar de 24/7 contactfunctie van de politie. Werkt deze contactfunctie zoals destijds was beoogd?[2] Wordt de minimum responstijd gehaald en hoeveel meldingen krijgt de politie hier dagelijks van binnen?

4. Financiële consequenties

De leden van de PVV-fractie lezen in de memorie van toelichting dat de verwachting is dat dit wetsvoorstel geen grote financiële gevolgen zal hebben en dat eventuele financiële consequenties zullen worden opgevangen binnen de begroting van het Ministerie van Veiligheid en Justitie. Op welke manier zullen deze eventuele financiële consequenties worden opgevangen en onder welke post op de begroting zal dit worden weggeschreven?

De voorzitter van de commissie,
Jadnanansing

Adjunct-griffier van de commissie,
Tielens-Tripels

[1] https://zoek.officielebekendmakingen.nl/ah-tk-20142015–202.html
[2] https://www.sp.nl/nieuws/2011/10/gesthuizen-krijgt-steun-voor-crashteam-ict-veiligheid