Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

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

772

Vragen van het lid **Sjoerdsma** (D66) aan de Minister van Buitenlandse Zaken over *Nederlanders die probeerden omstreden spionagesoftware te verkopen aan Ecuador* (ingezonden 22 november 2017).

Antwoord van Minister **Zijlstra** (Buitenlandse Zaken) (ontvangen 21 december 2017).

Vraag 1
Bent u bekend met het bericht «Deze Nederlanders probeerden omstreden spionagesoftware te verkopen»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe duidt u de activiteiten van het bedrijf Hacking Team, namelijk het verkopen van spionagesoftware aan repressieve regimes om journalisten, oppositieleden, activisten en anderen monddood te maken?

Antwoord 2
Vrijheid van meningsuiting is één van de prioriteiten binnen het Nederlands buitenlands mensenrechtenbeleid. De verkoop van deze producten door Hacking Team aan autoriteiten voor het ongelegitimeerd inperken van de vrijheid van meningsuiting keurt het kabinet af.

Vraag 3, 4, 5 en 6
Hoe duidt u het gegeven dat een Nederlandse honorair consul betrokken is geweest bij het faciliteren van een deal om spionagesoftware van het bedrijf Hacking Team te verkopen aan Ecuadoraanse inlichtingendiensten? Bent u op de hoogte van de activiteiten van deze honorair consul, zoals beschreven in het artikel? Zo ja, sinds wanneer? Welke acties heeft u vervolgens ondernomen? Acht u het wenselijk dat een vertegenwoordiger van de Nederlandse overheid in het buitenland betrokken is bij dergelijke nevenactiviteiten? Zo nee, welke acties onderneemt u om dergelijke praktijken te voorkomen? Zo ja, waarom? Klopt het dat de activiteiten van de honorair consul rondom het

[1] De Correspondent, 2 november 2017; https://decorrespondent.nl/7527/deze-nederlanders-probeerden-omstreden-spionagesoftware-te-verkopen/366542319-88b9df71

ah-tk-20172018-772
ISSN 0921 - 7398
's-Gravenhage 2017

promoten van dergelijke spionagesoftware volgens de geldende regelgeving niet gemeld hoefde te worden? Waarom niet? Acht u dit wenselijk?

Antwoord 3, 4, 5 en 6
Honorair consuls zijn onbezoldigde ambtenaren en worden geacht in hun levensonderhoud te voorzien middels andere activiteiten. Voordat een honorair consul wordt voorgedragen, is afgewogen wat de potentiële risico's van de beroepsmatige activiteiten van betrokkene zijn en worden doorgaans referenten geraadpleegd. De honorair consul is ambtenaar en behoort als zodanig tot de Dienst Buitenlandse Zaken. Op het gebied van integriteit gelden voor honorair consuls derhalve dezelfde normen als voor alle Rijksambtenaren. Zij worden daar bij hun aanstelling op gewezen. In de regelgeving is niet opgenomen dat een honorair consul economische activiteiten moet melden. Het is disproportioneel om honorair consuls te verplichten alle zakelijke activiteiten te melden. Wel is er continue aandacht voor integriteit en worden honorair consuls aangemoedigd om dilemma's bespreekbaar te maken.
Het Ministerie van Buitenlandse Zaken was niet op de hoogte van de samenwerking van de honorair consul met Hacking Team. De samenwerking tussen de honorair consul en Hacking Team vond plaats in zijn hoedanigheid van directeur van een handelsbedrijf. Het ministerie werd voor het eerst bekend met deze activiteiten op 4 juni 2017 toen de ambassade in Lima werd gewezen op het artikel op de website van PlanV. In januari 2017 was de benoemingsperiode van de honorair consul te Quito reeds afgelopen.

Vraag 7 en 8
Klopt het dat Hacking Team een demonstratie heeft gegeven over software aan de Nationale Politie en de Nederlandse militaire veiligheidsdienst? Waarom en op welk initiatief is dit gebeurd? Is hier vervolg aan gegeven? Zo ja, hoe? Wordt er momenteel of is er in het verleden door Nederlandse opsporingsdiensten op enigerlei wijze gebruik gemaakt van software van Hacking Team?

Antwoord 7 en 8
Zoals eerder is aangegeven in de beantwoording op de vragen van het lid Oosenbrug (PvdA) met kenmerk 2015Z09552 en Oosenbrug (PvdA) en Verhoeven (D66) met kenmerk 2015Z14018, brengt het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico's met zich mee voor de inzetbaarheid van die middelen. Dit geldt dus ook voor het verstrekken van informatie omtrent de broncode, de robuustheid en de daarmee samenhangende veiligheidsvraagstukken. Het kabinet kan hierover derhalve geen informatie over verstrekken. Het kabinet benadrukt dat er altijd wordt gehandeld binnen de bestaande wet- en regelgeving.
Voor het opsporen van bepaalde strafbare feiten kunnen op bevel van het Openbaar Ministerie (OM) bijzondere opsporingsbevoegdheden worden toegepast. Bij de inzet van dergelijke bevoegdheden dient het belang van de opsporing proportioneel te zijn aan de inbreuk die de bevoegdheid maakt op de persoonlijke levenssfeer van de verdachte of derden. Bovendien dient het te verkrijgen bewijs niet door de inzet van een andere, lichtere bevoegdheid te kunnen worden verkregen (subsidiariteit). Bij de inzet van ingrijpende bevoegdheden is machtiging van de rechter-commissaris vereist. De proportionaliteit en subsidiariteit van de inzet van de bevoegdheid, en het gebruik van het technisch hulpmiddel dat wordt ingezet ter uitvoering voor de bevoegdheid, worden hierbij getoetst.
Om de technologische ontwikkelingen op het gebied van cyber security bij te kunnen houden, onderhoudt de MIVD contacten met een groot aantal spelers in de publieke en private sector. Deze contacten lopen uiteen van het bezoeken van beurzen en congressen tot demonstraties van producten bij private partijen. Over mogelijke contacten van de MIVD met specifieke bedrijven worden in de regel geen mededelingen gedaan.

Vraag 9
Welke risico's ziet u voor cyberveiligheid in het bevorderen van het gebruik van dergelijke spionagesoftware?

Antwoord 9
Het kabinet stelt voorop dat het gebruik van dergelijke software niet wordt bevorderd van overheidswege. In algemene zin brengt digitalisering altijd risico's met zich mee en bevat software met regelmaat kwetsbaarheden. Dat is voor spionagesoftware niet anders. Dit onderwerp wordt reeds geadresseerd in het Cyber Security Beeld Nederland 2017. In lijn met de tweede Nationale Cyber Security en de Internationale Cyber Strategie kan aangegeven worden dat het altijd zoeken is naar een balans tussen vrijheid, veiligheid en maatschappelijke (of economische) groei. Deze balans komt ook terug in eerdere brieven (met o.a. het kenmerk 2008352) aan uw Kamer inzake de omgang met kwetsbaarheden in hard- en software.

Vraag 10
Klopt het dat in het Europees parlement het stelsel van vergunningen voor spionagesoftware momenteel wordt herzien zodat tussenhandel mogelijk strafbaar wordt? Wat is de Nederlandse opstelling hierin?

Antwoord 10
Op dit moment bespreken de Europese lidstaten het voorstel dat de Europese Commissie in september 2016 uitbracht voor de herziening van EU Verordening 428/2009. Deze verordening vormt het EU-raamwerk voor exportcontrole van dual-use goederen en tussenhandeldiensten voor dergelijke goederen. Tussenhandeldiensten voor dual-use goederen zijn op dit moment niet per se vergunningplichtig, maar kunnen dat wel zijn. Om dit te beoordelen dienen Nederlandse bedrijven een mededeling te doen van de tussenhandeldiensten die zij voornemens zijn te plegen. Nederland acht een dwingende vergunningplicht voor alle tussenhandeldiensten voor dual-use goederen onwenselijk, maar wil wel zicht hebben op de te plegen tussenhandeldiensten om deze eventueel vergunningplichtig te verklaren. In haar voorstel breidt de Commissie de definitie van tussenhandelaar uit tot bedrijven die gelieerd zijn aan een in de EU gevestigde onderneming, maar zich buiten de EU bevinden. Daarmee wil de Commissie de rechtsmacht van de EU exportcontrole autoriteiten vergroten. Nederland hecht in de onderhandelingen over het voorstel van de Commissie aan regels die helder zijn richting het bedrijfsleven en aan de uitvoerbaarheid van deze regels.