Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

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

393

Vragen van het lid **Verhoeven** (D66) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat over *het bericht «Australische overheid verbiedt Huawei en ZTE apparatuur te leveren voor 5g»* (ingezonden 18 september 2018).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens Staatssecretaris **Keijzer** (Economische Zaken en Klimaat) (ontvangen 18 oktober 2018). Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 214.

Vraag 1
Bent u bekend met het bericht «Australische overheid verbiedt Huawei en ZTE apparatuur te leveren voor 5G» en de verklaring van de Australische overheid?[1]

Antwoord 1
Ja.

Vraag 2
Onderschrijft u het grote economische en maatschappelijke belang van 5G op het gebied van connectiviteit en communicatie voor bedrijven en burgers, het belang van 5G voor vitale (toekomstige) systemen op het gebied van mobiliteit, elektriciteit en zorg en het belang voor de ontwikkeling van het Internet of Things?

Antwoord 2
Ja.

Vraag 3
Aangezien zowel Australië als de Verenigde Staten en het Verenigd Koninkrijk hebben maatregelen genomen om de nationale veiligheid van dergelijke vitale infrastructuur te garanderen, bent u in contact met deze landen over de genomen besluiten en de informatie waarop deze besluiten zijn genomen? Is er aanleiding om een dergelijk besluit ook voor Nederland te nemen?

[1] https://tweakers.net/nieuws/142463/australische-overheid-verbiedt-huawei-en-zte-apparatuur-te-leveren-voor-5g.html, https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

ah-tk-20182019-393
ISSN 0921 - 7398
's-Gravenhage 2018

Antwoord 3
Uiteraard heeft het kabinet aandacht voor ontwikkelingen in technologieën en kwetsbaarheden daarin en voor de noodzaak scherp te blijven op de beveiliging hiervan. Ook de internationale ontwikkelingen rond Chinese technologiebedrijven worden door het kabinet gevolgd.
Nederland maakt een eigenstandige afweging. De Nederlandse overheid beziet de risico's die verbonden zijn aan dergelijke producten en bedrijven op een zorgvuldige «case by case» basis, waarbij in ieder geval de volgende criteria worden betrokken:
– is er sprake van een statelijke actor die zich richt tegen Nederlandse belangen?
– is er sprake van wetgeving die een bedrijf verplicht om op enigerlei wijze samen te werken met die betreffende actor?

Gezien de nationale veiligheidsbelangen en de belangen van het bedrijfsleven wordt niet vooruitgelopen of gespeculeerd over al dan niet mogelijke toekomstige maatregelen.

Vraag 4
Wat is uw reactie op de vier eisen aan het 5G-netwerk die de Australische regering formuleert in haar verklaring over deze kwestie? Bent u het eens met de analyse van de Australische regering over het vervagen van grenzen tussen «rand» en «kern»-apparatuur bij 5G?

Antwoord 4
5G heeft inderdaad een architectuur die verschilt van die van de huidige generatie mobiele netwerken. Op basis van een analyse van de risico's die dat met zich meebrengt wordt een afweging gemaakt van mogelijke toekomstige maatregelen. Ieder land maakt daarbij zijn eigen risico-afweging, zoals Australië dat heeft gedaan met zijn eisen, en de Nederlandse overheid eveneens een eigen afweging maakt.

Vraag 5
In hoeverre valt de hardware van bedrijven als Huawei en ZTE binnen het in de brief over Kaspersky virussoftware geformuleerde kader (Kamerstuk 30 821, nr. 46), namelijk: a) diepgaande toegang tot ICT-systemen, b) een plicht tot het navolgen van buitenlandse wetgeving (in dat geval Russische) en c) een offensief cyberprogramma van dat betreffende land?

Antwoord 5
Gezien de nationale veiligheidsbelangen en de belangen van het bedrijfsleven wordt niet vooruitgelopen op of gespeculeerd over welke producten, diensten of bedrijven al dan niet een risico zouden kunnen vormen voor de nationale veiligheid en over al dan niet mogelijke toekomstige maatregelen.

Vraag 6
Op welke manier geschiedt de besluitvorming om tot dergelijke besluiten, zoals met de antivirussoftware van Kaspersky, te komen? Ziet u reden om een uitgebreider kader op te stellen om dergelijke besluiten van nationale veiligheid te nemen?

Antwoord 6
De Nederlandse overheid beziet de risico's die verbonden zijn aan dergelijke producten en bedrijven op een zorgvuldige «case by case» basis, waarbij in ieder geval de volgende criteria worden betrokken:
– is er sprake van een statelijke actor die zich richt tegen Nederlandse belangen?
– is er sprake van wetgeving die een bedrijf verplicht om op enigerlei wijze samen te werken met die betreffende actor?

Omdat elke casus specifieke kenmerken heeft, biedt het huidige kader voldoende flexibiliteit om bij elke afzonderlijke casus een analyse naar de eventuele risico's voor de nationale veiligheid uit te voeren.

Vraag 7
Op wat voor manier vindt er Europese samenwerking op dergelijke kwesties van nationale veiligheid plaats? Vindt u het wenselijk als er ook op Europees niveau strategisch vanuit nationaal veiligheidsbelang gekeken wordt naar dergelijke kwesties?

Antwoord 7
Nationale veiligheid is een primaire verantwoordelijkheid van de lidstaten. Echter faciliteert de EU samenwerking tussen lidstaten op het gebied van veiligheid, bijvoorbeeld middels werkgroepen waarin kennis, informatie en «best practices» worden uitgewisseld over dergelijke onderwerpen. Nederland acht het van belang dat informatie en kennis wordt uitgewisseld over dergelijke onderwerpen in EU-verband, hierbij is het echter van belang dat de nationale competentie van nationale veiligheid wordt gerespecteerd.