

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

3918

Vragen van het lid **Buitenweg** (GroenLinks) aan de Minister van Justitie en Veiligheid over *het besluit van de Britse regering om Huawei volledig uit te sluiten van het Britse 5G-netwerk* (ingezonden 17 juli 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 28 augustus 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 3687.

Vraag 1

Heeft u kennisgenomen van het bericht «Huawei alsnog weg uit Brits 5G»?¹

Antwoord 1

Ja.

Vraag 2

Deelt u de mening dat de Britse inlichtingendiensten een bijzondere kennispositie over Huawei op hebben kunnen bouwen de afgelopen jaren vanwege hun nauwe samenwerking met het bedrijf in de Huawei Cyber Security Evaluation Centre (HCSEC), dat in 2010 is opgezet?

Antwoord 2

Het VK doet al sinds 2010 onderzoek naar de kwaliteit van de producten van Huawei in het Huawei Cyber Security Evaluation Centre. Over deze onderzoeken brengt het VK geregeld openbare rapporten naar buiten. Over de kennispositie van inlichtingendiensten worden in het openbaar geen uitspraken gedaan.

Vraag 3, 4

Wat is uw reactie op de recente verandering van het Britse beleid ten aanzien van het gebruik van Huawei apparatuur in het Britse 5G-netwerk?

Wat is uw reactie op de stelling van de Britse Minister van Digitalisering Oliver Dowden, dat de Amerikaanse sancties Huawei dwingen om uit te wijken naar Aziatische toeleveranciers en op zijn uitspraak geen vertrouwen te hebben in die alternatieven? Heeft u dat vertrouwen wel? Zo ja, op welke

¹ NRC van 15 juli 2020

basis? Zo nee, wat betekent dat voor het Nederlandse beleid ten aanzien van het gebruik van Huawei-apparatuur in het 5G-netwerk?

Antwoord 3, 4

Ik volg de ontwikkelingen in het beleid ten aanzien van het 5G-netwerk in het Verenigd Koninkrijk op de voet, inclusief de overwegingen om Huawei volledig uit te sluiten van het Britse 5G-netwerk.

Ik wil benadrukken dat Nederland een eigenstandige afweging maakt met betrekking tot de veiligheid en integriteit van de telecomnetwerken. Eén van de maatregelen die het kabinet heeft genomen naar aanleiding van deze risicoanalyse is het inrichten van een structureel proces waar nieuwe informatie over dreiging en technologie wordt beoordeeld door overheid en de telecomsector.² Indien nodig worden op basis hiervan aanvullende maatregelen genomen. Op deze manier worden de telecomnetwerken ook in de toekomst beschermd tegen dreigingen. Binnen dit structurele proces worden alle relevante ontwikkelingen rondom de telecomnetwerken meegenomen.

Vraag 5

Kunt u een overzicht geven van alle Amerikaanse sancties die zijn ingesteld tegen Huawei sinds begin 2019? Welke effecten hebben die maatregelen nu al op de bedrijfsvoering en welke effecten zijn te verwachten voor de toekomst?

Antwoord 5

Voor zover bekend wordt Huawei geraakt door de volgende sinds begin 2019 afgekondigde sancties en andersoortige beperkende maatregelen:

Mei 2019 – plaatsing Huawei op de zgn. Entity List: deze lijst wordt door de VS gebruikt om export naar op de lijst geplaatste entiteiten en individuen onder controle te brengen en de facto te blokkeren tenzij een licentie wordt verleend door de VS. Er geldt momenteel alleen nog een tijdelijke licentie uitzondering voor beperkt typen transacties aan Huawei gericht op onderzoek en het verantwoord ontsluiten van cybersecurity kwetsbaarheden.

Mei en augustus 2020 – Amendementen op de Foreign-Produced Direct Product Rule. Deze regel beschrijft een breed spectrum aan transacties die de VS onder controle brengt met het doel Huawei de mogelijkheid te ontzeggen gebruik te maken van high-end chip sets die zijn ontwikkeld dan wel geproduceerd m.b.v. Amerikaanse technologie of software. Vanaf 15 september a.s. treedt de regel in werking waarna organisaties en bedrijven die transacties aangaan die (in)direct in verband staan met Huawei, verplicht worden een licentie aan te vragen bij het Commerce Department.

Juli 2020 – Visa Restrictions on Certain Employees of Chinese Technology Companies that Abuse Human Rights. Het gaat hier om visabeperkingen voor specifieke werknemers van een aantal Chinese technologiebedrijven waaronder Huawei.

De mobiele netwerkaanbieders geven aan dat de maatregelen vooralsnog een beperkte invloed op de bedrijfsvoering hebben en dat zij maatregelen nemen om de impact te minimaliseren.

Vraag 6

Heeft u de Taskforce Economische Veiligheid gevraagd om de nationale risicoanalyse 5G te actualiseren naar aanleiding van de recente ontwikkelingen in de wereldwijde technologiemarkt, zoals de Amerikaanse sancties tegen Huawei en andere Chinese bedrijven? Zo nee, bent u bereid om dat alsnog te doen?

Antwoord 6

De huidige internationale ontwikkelingen worden scherp in de gaten gehouden en gemonitord op de eventuele effecten voor de sector. Zoals aangegeven bij antwoord 4 is één van de maatregelen die het kabinet heeft genomen het inrichten van een structureel proces. Daarbij vindt continue beoordeling plaats van ontwikkelingen in dreiging en technologie. Hierbij wordt het effect op de weerbaarheid van de telecomnetwerken in kaart

² Kamerstuk 30 821, nr. 92

gebracht. Dit kan aanleiding zijn voor het nemen van aanvullende beveiligingsmaatregelen.

Geopolitieke en technologische ontwikkelingen worden hierin, net als alle andere ontwikkelingen, meegenomen.

Vraag 7

Heeft u ten aanzien van andere EU-lidstaten aanwijzingen ontvangen over een mogelijke herziening in de besluitvorming over samenwerking met Huawei in de uitrol van het 5G-netwerk? Kunt u daarbij toelichten hoe deze discussie in de EU en de NAVO verloopt en of er eventuele gevolgen zijn verbonden aan het besluit van het Verenigd Koninkrijk voor wat betreft de onderlinge samenwerking op het gebied van inlichtingen en veiligheid?

Antwoord 7

Net als Nederland volgen de andere EU-lidstaten de recente ontwikkelingen in de wereldwijde technologiemarkt, zoals de Amerikaanse sancties tegen Huawei en andere Chinese bedrijven. We hebben geen aanwijzingen ontvangen over een mogelijke herziening in de besluitvorming over samenwerking met Huawei in de uitrol van het 5G-netwerk in andere EU-lidstaten. De EU heeft in januari van dit jaar de EU 5G Toolbox aangenomen om te zorgen voor een veilige uitrol van het 5G netwerk.³ De discussie in EU verband vindt plaats in de het periodiek overleg dat plaats vindt in het kader van de Network and Information Security Directive. Ook de NAVO heeft aandacht voor de veiligheid van telecommunicatienetwerken, waaronder 5G.⁴ De verantwoordelijkheid ligt bij de individuele landen. Over de aard en de inhoud van contacten met andere inlichtingendiensten kunnen in de openbaarheid geen mededelingen worden gedaan.

Vraag 8

Wanneer verwacht u de ministeriële regelingen af te kondigen om nader invulling te geven aan het «Besluit veiligheid en integriteit telecommunicatie» van 5 december 2019? Op welke basis wordt besloten welke leveranciers gelden als vertrouwde leveranciers?

Antwoord 8

Er wordt momenteel een concept ministeriële regeling opgesteld waarin de technische en organisatorische beveiligingsmaatregelen worden opgenomen. Deze zal vervolgens worden geconsulteerd. Daarna zal de conceptregeling moeten worden genotificeerd bij de Europese Commissie. Na afloop van deze notificatieprocedure zal de regeling worden vastgesteld en worden gepubliceerd. Dit zal naar verwachting begin 2021 geschieden.

Op grond van het Besluit veiligheid en integriteit telecommunicatie is de Minister van Economische zaken, in overleg met de Minister van Justitie en Veiligheid bevoegd, een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst een verplichting op te leggen om in de daarbij aangewezen onderdelen van diens netwerk of bijbehorende faciliteiten, uitsluitend gebruik te maken van producten of diensten van anderen dan de daarbij door de Minister genoemde partij.

Dit kan alleen indien dat noodzakelijk is om risico's voor de veiligheid en integriteit van diens netwerk of dienst die de nationale veiligheid of de openbare orde raken te beheersen. De criteria hiervoor staan opgenomen in de AMvB.⁵ Er wordt op basis hiervan bepaald of er niet-vertrouwde leveranciers zijn. Het proces is niet gericht op het selecteren van vertrouwde leveranciers.

³ <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

⁴ London declaration, 4 december 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm

⁵ Een partij kan worden aangewezen wanneer die deze: (a) een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft een in Nederland aangeboden elektronisch communicatienetwerk of -dienst te misbruiken of uit te laten vallen, of (b) nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld onder a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

Vraag 9

Vormen de recente ontwikkelingen met betrekking tot Hong Kong en de *National Security Law*, die via Artikel 38 ook een extraterritoriale component heeft, reden om het vertrouwen in Chinese bedrijven met nauwe banden met de Chinese overheid te herzien?

Antwoord 9

Er is niet een direct verband tussen de invoering van de Nationale Veiligheidswet in Hongkong en het vertrouwen in Chinese bedrijven met nauwe banden met de Chinese overheid.