Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

1515

Vragen van de leden **Buitenweg** en **Bromet** (beiden GroenLinks) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat over *de veiligheid van het 5G netwerk* (ingezonden 25 november 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 28 januari 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 1164.

Vraag 1
Bent u bekend met het bericht «EU poised to send warning to China on 5G» van Bloomberg?[1]

Antwoord 1
Ja.

Vraag 2
Bent u het eens met de stelling dat de beoordeling van de leveranciers van 5G infrastructuur ook moet kijken naar de nationale wetgeving in het land waar de leverancier vandaan komt, en dan met name of daar bepalingen in staan die de leverancier kunnen dwingen tot het delen van data met de lokale autoriteiten? Zo ja, kan de aanwezigheid van dergelijke bepalingen reden zijn om de leverancier niet goed te keuren? Zo nee, waarom niet?

Antwoord 2
In het Besluit veiligheid en integriteit telecommunicatie[2], zoals dat op 5 december 2019 is gepubliceerd, wordt geregeld dat aanbieders van openbare elektronische communicatie netwerken of -diensten in Nederland de verplichting kan worden opgelegd om in de kritieke onderdelen van hun netwerken louter gebruik te maken van producten of diensten van anderen dan de daarbij genoemde, voor die kritieke onderdelen uitgesloten, leveranciers. Daarbij gelden krachtens dit besluit als criteria voor het uitsluiten van leveranciers, dat bekend is of gronden zijn te vermoeden dat de genoemde leveranciers de intentie hebben om Nederlandse telecomnetwerken te

[1] Bloomberg, 19 november 2019, https://www.bloomberg.com/news/articles/2019-11-19/eu-says-politics-matter-for-5g-suppliers-in-message-to-china
[2] Staatsblad 2019, nr. 457.

ah-tk-20192020-1515
ISSN 0921 - 7398
's-Gravenhage 2020

misbruiken of te laten uitvallen, dan wel dat zij nauwe banden hebben met of onder invloed staan van een partij met die intentie.
Zoals toegelicht bij het Besluit veiligheid en integriteit telecommunicatie zijn deze criteria in lijn met de overwegingen die het kabinet hanteert bij de beoordeling van risico's ten aanzien van onder meer spionage door statelijke actoren, zoals die zijn vermeld in de brief aan de Tweede Kamer over C2000.[3] Dat betekent dat bij de beoordeling van bovengenoemde leveranciers ook wordt gekeken naar de wetgeving van het land waaruit de leverancier afkomstig is, en meer in het bijzonder of deze wetgeving de leverancier verplicht om (bv. in de vorm van het moeten delen van data) samen te werken met de overheid van dat land.

Vraag 3, 4
Bent u het eens met de risicobeoordeling van de Europese Unie (EU) dat ook delen van het netwerk buiten de kern, zoals het Radio Access Network (RAN), moeten worden bestempeld als «hoog risico» voor spionage en sabotage en worden de extra veiligheidseisen ook van toepassing op het RAN? Zo ja, hoe beoordeelt u het feit dat Nederlandse providers al investeren in Chinese technologie in dit deel van het netwerk, terwijl de extra veiligheidseisen nog niet zijn afgekondigd? Zo nee, waarom niet?
Zullen alle delen van 5G die beoordeeld worden als «hoog risico» ook expliciet zo worden benoemd? Of klopt het, zoals de Minister van Justitie en Veiligheid suggereerde tijdens het algemeen overleg over nationale veiligheid en crisisbeheersing van 14 november jl. dat dit niet bekend kan worden gemaakt vanwege redenen die samenhangen met nationale veiligheid?

Antwoord 3, 4
De Taskforce Economische Veiligheid heeft in de nationale risicoanalyse op basis van de te beschermen belangen en de actuele dreiging kritieke onderdelen geïdentificeerd in de huidige telecomnetwerken. De lijst met kritieke onderdelen is als vertrouwelijk geclassificeerd en kan ik daarom niet met u delen.
In samenwerking met de telecomaanbieders wordt een structureel proces ingericht. Deze structurele aanpak maakt het mogelijk om adaptief te kunnen reageren op veranderingen in de dreiging of ontwikkelingen in de telecomnetwerken. Op die manier kunnen ook de telecomnetwerken in de toekomst beschermd worden tegen de dreiging.
Nederland heeft actief bijgedragen aan de totstandkoming van de Europese risicoanalyse, die zich richt op het toekomstige 5G netwerk, en de bevindingen zijn in lijn met en complementair aan de bevindingen van de Nederlandse Taskforce Economische Veiligheid.
De telecomaanbieders zijn geïnformeerd over de maatregelen die het kabinet neemt. De telecomaanbieders blijven ook bij de nadere uitwerking hiervan nauw betrokken en het is daarbij aan deze partijen om bij hun investeringen hier rekening mee te houden.

Vraag 5
Bent u het eens met de stelling dat het 5G netwerk in de Europese Unie moet zijn gegrond op de basiswaarden van de EU, zoals mensenrechten, de rechtsstaat en het beschermen van privacy? Zo ja, worden deze principes meegenomen in de beoordeling van leveranciers? Zo nee, waarom niet?

Antwoord 5
Zoals bij alle telecommunicatienetwerken is het belangrijk dat ook bij 5G-netwerken de randvoorwaarden zijn geborgd. De Telecommunicatiewet, waarin de Europese richtlijnen op het gebied van telecommunicatie en e-privacy zijn geïmplementeerd, biedt deze borging op tal van onderwerpen, waaronder de privacy, vertrouwelijkheid, veiligheid en integriteit. Deze regels richten zich tot de openbare aanbieders van elektronische communicatienetwerken en -diensten. Zij zijn op grond van artikel 11a.1 van de Telecommunicatiewet verplicht passende technische en organisatorische maatregelen te nemen om de risico's voor de integriteit en veiligheid van hun netwerken en -diensten te beheersen. Het Besluit veiligheid en integriteit telecommunicatie,

[3] Kamerstuk 25 124, nr. 96

dat hierop is gebaseerd, biedt de mogelijkheid om telecomaanbieders daarbij te verplichten in de kritieke onderdelen van hun netwerken uitsluitend gebruik te maken van producten en diensten van vertrouwde leveranciers. Zoals hierboven ook in het antwoord op vraag 2 vermeld, zal het criterium bij de beoordeling van leveranciers zijn of zij zelf de intentie hebben om Nederlandse telecomnetwerken te misbruiken of laten uitvallen, dan wel nauwe banden hebben met of onder invloed staan van een partij met die intentie. Bij misbruik valt te denken aan spionage: ongeoorloofde toegang tot communicatiegegevens, zowel verkeersgegevens als inhoud van communicatie. Daarnaast zijn de aanbieders uiteraard ook gehouden aan de privacyregels in de Telecommunicatiewet en de Algemene verordening gegevensbescherming. Verder zijn er ook algemenere kaders zoals het Europees Verdrag voor de Rechten van de Mens.»

Vraag 6
Kunt u zich vinden in de laatste aanbeveling van de EU risicobeoordeling dat de EU en haar lidstaten bij de uitrol van het 5G-netwerk ook rekening moeten houden met de ontwikkeling van de eigen industriële capaciteit op het gebied van 5G? Zo ja, hoe bent u van plan om deze aanbeveling op te volgen? Zo nee, waarom niet?

Antwoord 6
Het is belangrijk om het vraagstuk van industriële capaciteit voor 5G te bezien in een bredere context van innovatiebeleid, omdat dit vraagstuk ook op andere terreinen speelt. Om de transitie naar een duurzame en digitale economie te kunnen maken is een stevig innovatiebeleid nodig. Gezamenlijk optrekken binnen de EU zal ontwikkeling van sleuteltechnologieën en onderzoek en innovatie in het algemeen bevorderen. Ook het versterken van de Europese interne markt heeft onze blijvende prioriteit. Hierbij is het vooral belangrijk om uit te blijven gaan van onze eigen economische waarden. Open markten zorgen ervoor dat onze bedrijven concurrerend en innovatief zijn en leveren nieuwe producten en diensten op voor consumenten, tegen redelijke prijzen. Binnen de interne markt zijn strenge mededingingsregels en politiek onafhankelijk toezicht nodig voor het beschermen van de belangen van de consument en het faciliteren van eerlijke concurrentie. Over de aspecten waarop een eventuele stimulering van de eigen 5G industriële capaciteit plaatsvindt en de mate waarin dat dan gebeurt wordt nog in EU-verband besproken.