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

37

Vragen van de leden **Buitenweg** en **Bromet** (beiden GroenLinks) aan de Ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties over *het advies van de AIVD over de nationale veiligheid en veiling 5G* (ingezonden 16 juli 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie (ontvangen 18 september 2019). Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3559.

Vraag 1 en 2
Wat is de reden dat de brief van de AIVD over nationale veiligheid en 5G, van 4 februari 2019, niet al in februari is doorgestuurd naar de Tweede Kamer? Wat is de reden dat de brief van de AIVD niet werd toegezonden als bijlage bij uw brief aan de Tweede Kamer van 1 juli 2019 over maatregelen ter bescherming van telecomnetwerken en 5G?[1]

Antwoord 1 en 2
De brief van de AIVD en de MIVD betreft een eerste duiding ten aanzien van de veiligheidsvraagstukken rond de 5G telecominfrastructuur. De brief is meegenomen en meegewogen bij de nadere analyses die zijn uitgevoerd in het kader van de risicoanalyse van de Taskforce. Op basis van deze risicoanalyse is de Taskforce tot haar advies gekomen dat mede door de AIVD en de MIVD, als leden van de Taskforce, is opgesteld.
Omdat de brief van de AIVD en de MIVD één onderdeel is van het analyseproces van de Taskforce is er voor gekozen de brief niet los en buiten de context van de rapportage aan de Kamer te sturen. Begin juli 2019 is de brief van de AIVD en de MIVD als bijlage toegevoegd aan de rapportage van de Taskforce en onderdeel geweest van de vertrouwelijke briefing aan uw Kamer. Voorafgaand aan de briefing en het plenair debat over 5G is leden van de vaste Kamercommissie van Justitie en Veiligheid en van Economische Zaken en Klimaat de mogelijkheid geboden de rapportage van de Taskforce en de brief vertrouwelijk in te zien. Op 8 juli jl. is de brief, naar aanleiding van berichtgeving in de Volkskrant, (ditmaal separaat) aan uw Kamer aangeboden.[2]

[1] Maatregelen bescherming telecomnetwerken en 5G (2019Z13859)
[2] Kamerstuk 30 821, nr. 89.

ah-tk-20192020-37
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 3
Wat is het beleid met betrekking tot het doorgeleiden van AIVD-adviezen? Wie neemt de beslissing een advies al dan niet aan de Tweede Kamer toe te zenden?

Antwoord 3
Bij de grondwetswijziging in 1983 is door de regering betoogd dat bewindspersonen het parlement uit eigen beweging moeten informeren wanneer «dat in het belang van een goede en democratische bestuursvoering wenselijk is».[3] De bewindspersonen die het advies hebben ontvangen hebben in dit geval besloten dat het wenselijk is uw Kamer te informeren. Hoe en in welke context de Kamer geïnformeerd is over de brief van de AIVD en MIVD leest u terug onder de beantwoording van vraag 1 en 2.

Vraag 4
Herinnert u zich de brief Beveiliging nieuwe infrastructuur mobiele communicatie (C2000) (Kamerstuk 25 124, nr. 96)? Deelt u de constatering dat deze brief expliciet ingaat op de adviezen van de AIVD inzake C2000, zoals verwoord in de brief van de AIVD van 17 januari 2019?[4]

Antwoord 4
Ja deze brief herinner ik mij. In de brief wordt expliciet verwezen naar de adviezen van de AIVD inzake C2000 zoals verwoord in de bijlage ««Beantwoording adviesopdracht C2000»»[5] van de AIVD van 17 januari 2019.

Vraag 5
Waarom gaat de brief van 1 juli over 5G niet expliciet in op de aanbevelingen van de AIVD zoals verwoord in de brief van 4 februari 2019?

Antwoord 5
De Taskforce heeft een eigenstandige risicoanalyse uitgevoerd waarbij alle deelnemers betrokken zijn geweest en hun expertise hebben geleverd. Er is daarbij rekening gehouden met zowel veiligheids- als economische belangen. De brief van de AIVD en de MIVD is meegenomen en meegewogen bij de risicoanalyse van de Taskforce. De Taskforce heeft een eigenstandig advies opgesteld. De AIVD en de MIVD zijn deelnemers van de Taskforce en onderschrijven, net als de andere taskforce-leden, de voorgestelde aanpak.

Vraag 6, 7 en 8
Hoe beoordeelt u het advies van de AIVD (nummer 3 in de brief) om «een aanpak te formuleren voor het uitfaseren van bepaalde hard- en software binnen de kritieke belangen in de bestaande telecom infrastructuur (2G, 3G, 4G) afkomstig van dienstverleners uit landen met een offensief cyberprogramma»? Bent u van plan deze aanbeveling op te volgen?
Hoe beoordeelt u het advies van de AIVD (nummer 4 in de brief) om nieuwe afhankelijkheden in de 5G infrastructuur te voorkomen, «door bepaalde hard- en software van dienstverleners uit landen met een offensief cyberprogramma selectief te weren»? Hoe verhoudt dit advies zich tot uw uitspraken in het plenaire debat over de uitrol van 5G dat u kiest voor een landenneutraal uitgangspunt?
Klopt het dat u in uw brief van 26 april 2019 over C2000 schrijft dat u het advies van de AIVD om zo snel mogelijk over te gaan teneinde te komen tot een oplossing waarbij de afhankelijkheid van ICT-systemen uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma voeren tegen Nederlandse belangen overneemt? Neemt u alle 8 de adviezen van de AIVD over 5G ook over, zo nee, welke niet?

Antwoord 6, 7 en 8
De brief van de AIVD en de MIVD van februari 2019, is meegenomen en meegewogen bij de risicoanalyse van de Taskforce. Op basis van deze risicoanalyse worden verschillende maatregelen genomen, zoals ook gemeld

[3] Kamerstuk 19 014, nr. 5 (MvA), blz. 6.
[4] Beantwoording adviesopdracht C2000 (bijlage bij Kamerstuk 25 124, nr. 96)
[5] Kamerstuk 25 124, nr.

aan uw kamer.[6] De AIVD en MIVD zijn deelnemers van de Taskforce en onderschrijven, net als de andere Taskforce-leden, de voorgestelde aanpak. Deze maatregelen geven een adequaat antwoord op de dreiging en zijn van toepassing op de huidige en toekomstige netwerken. De noodzakelijke aanscherpingen van de eisen die worden gesteld aan de veiligheid en integriteit van de mobiele telecommunicatienetwerken zullen in nadere regelgeving worden vastgelegd en zal dit najaar worden gepubliceerd.
De aanpak van het kabinet is landenneutraal. Dit betekent dat elke leverancier – ongeacht land van herkomst – moet voldoen aan de extra hoge eisen die worden gesteld aan leveranciers van diensten en producten in de kritieke onderdelen van de telecomnetwerken.
De AIVD adviseert inzake C2000 om parallel aan de migratie te starten met een vervangingstraject waarbij de afhankelijkheid van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen is geminimaliseerd. Ik neem dit advies over zoals aangegeven in mijn brief van 26 april jl.[7] en heb onmiddellijk opdracht gegeven tot een verkenning naar een dergelijke oplossing. Ik zal uw Kamer hierover na de zomer informeren, dit heb ik tijdens het AO Nationale Veiligheid en Crisisbeheersing van 20 juni jl. bevestigd. Hierbij hecht ik er aan om uw Kamer er op te wijzen dat de veiligheid van C2000 en 5G andersoortige vraagstukken zijn die om andersoortige oplossingen vragen en derhalve is een ander proces doorlopen.[8]

Vraag 9
Hoe beoordeelt u het advies van Professor Bart Jacobs van de Radboud Universiteit Nijmegen om met betrekking tot 5G van alle leveranciers open source software te verlangen, zoals verwoord in zijn brief van 2 april 2019 over de vernieuwing C2000?[9] Bent u van plan dat advies op te volgen?

Antwoord 9
Professor Bart Jacobs heeft in zijn advies de vrijblijvende suggestie gedaan dat Nederland en Europa er goed aan zouden doen om collectief met betrekking tot 5G open source software van (alle) leveranciers te verlangen. Een dergelijke oplossingsrichting is er een van de lange termijn en zou indien wenselijk vorm moeten krijgen binnen een bredere Europese aanpak. Zoals u weet steunt het kabinet een Europese aanpak waar risicoanalyses en oplossingsrichtingen tussen lidstaten worden gedeeld. Het Europese traject naar aanleiding van de aanbeveling «»Cyberbeveiliging van 5G-netwerken»» moet resulteren in een instrumentarium dat maatregelen bevat om (nationaal) geïdentificeerde risico's te kunnen aanpakken. Het instrumentarium wordt momenteel door de Lidstaten en de Commissie ontwikkeld.

---

[6] Maatregelen bescherming telecomnetwerken en 5G
[7] Kamerstuk 25 124 en 29 628, nr. 92
[8] Kamerstuk 25 124 en 24 095, nr. 94
[9] Advisering m.b.t. vernieuwing C2000 (bijlage bij Kamerstuk 25 124, nr. 96)