

Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Minister van Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk

2355936

Uw kenmerk

2018Z14691

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 24 september 2018
Onderwerp Antwoorden Kamervragen over artikel 'New defense bill bans the U.S.
government from using Huawei and ZTE tech'

In antwoord op uw brief van 17 augustus 2018 deel ik u mee, dat de schriftelijke vragen van het lid Arno Rutte (VVD) over het artikel 'New defense bill bans the U.S. government from using Huawei and ZTE tech' worden beantwoord zoals aangegeven in de bijlage van deze brief.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

Antwoorden van de Minister van Justitie en Veiligheid op schriftelijke vragen van het lid Arno Rutte (VVD) over het artikel 'New defense bill bans the U.S. government from using Huawei and ZTE tech' (ingezonden 17 augustus 2018, 2018Z14691)

Minister van Justitie en Veiligheid

Datum
24 september 2018

Ons kenmerk
2355936

Vraag 1

Kent u het artikel 'New defense bill bans the U.S. government from using Huawei and ZTE tech'? 1)

Antwoord op vraag 1

Ja.

Vraag 2

Deelt u de analyse van de Amerikaanse regering dat het gebruik van Chinese apparatuur van 2 bepaalde fabrikanten, daar waar het gaat om een 'substantieel of essentieel onderdeel van een systeem, evenals technologie die gebruikt wordt voor het routeren of bekijken van gebruikersdata' een gevaar kan vormen voor de nationale veiligheid en daarom verboden wordt? Zo ja, welke maatregelen gaan er door u genomen worden en op welke termijn? Zo nee, waarom is de Nederlandse veiligheidsafweging anders dan de Amerikaanse veiligheidsafweging?

Antwoord op vraag 2

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?

Nederland maakt hierin een eigenstandige afweging. Gezien de nationale veiligheidsbelangen en de belangen van het bedrijfsleven wordt niet vooruitgelopen of gespeculeerd over al dan niet mogelijke toekomstige maatregelen.

Vraag 3

Heeft u kennisgenomen van het feit dat het in het artikel genoemde verbod ook geldt voor Hytera, het bedrijf dat de technologie voor het netwerk en de portofoons voor C2000 levert?

Antwoord op vraag 3

Ja.

Vraag 4

Als in de Verenigde Staten het gebruik van technologie van Hytera voor communicatiediensten van de overheid als een gevaar voor de nationale veiligheid wordt gezien, hoe kan de Nederlandse nationale veiligheid dan na ingebruikname van het nieuwe C2000 wél gewaarborgd zijn?

Antwoord op vraag 4

Zoals eerder aan uw Kamer is gemeld¹ wordt C2000 gebruikt voor de reguliere communicatie tussen de hulpverleningsdiensten: politie, brandweer, ambulance en Koninklijke Marechaussee. Het beveiligingsniveau voor deze gebruikersgroepen is bepaald op het niveau "departementaal vertrouwelijk". Ook het beveiligingsniveau van het vernieuwde netwerk zal als zodanig worden ingericht. De communicatie via het C2000-netwerk is versleuteld en maakt gebruik van afgeschermdde verbindingen. Er zijn bij het classificatieniveau passende maatregelen genomen om sabotage te herkennen en te voorkomen. Versleuteling gebeurt door de leveranciers van de randapparatuur en deze versleuteling wordt door de politie in het netwerk gezet. Gebruikers bepalen zelf de leveranciers van de randapparatuur. Gebruikers kunnen extra versleuteling toepassen indien nodig.

Gelet op de vragen die zijn gerezen door de betrokkenheid van een Chinese aandeelhouder bij de ontwikkeling van C2000 heb ik Xebia gevraagd om een security audit uit te voeren op de technische ICT-oplossing die Hytera als onderdeel van de vernieuwing van C2000 realiseert. Daarnaast ben ik in gesprek met het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD om mij hierover te adviseren. Ik zal passende maatregelen nemen wanneer daartoe aanleiding is.

Uiteraard houd ik de veiligheid van de systemen die gebruikt worden goed in de gaten en heeft het kabinet aandacht voor ontwikkelingen in technologieën en kwetsbaarheden daarin, en de noodzaak scherp te blijven op de beveiliging hiervan. Ook de internationale ontwikkelingen rond Chinese technologiebedrijven worden door mijn departement gevolgd.

Vraag 5

Overweegt u, in navolging op het verbod op Kaspersky software bij overheidsdiensten, ook in Nederland een verbod op het gebruik van essentiële diensten van Chinese makelij? Zo ja, welke consequenties heeft zo'n besluit voor de korte en de middellange termijn, in het bijzonder met het oog op C2000? Zo nee, waarom niet?

Antwoord op vraag 5

Zie het antwoord op vraag 2.

Het dreigingsbeeld op het terrein van digitale risico's heeft geleid tot een aangescherpte afweging ten aanzien van het gebruik van specifieke digitale producten en diensten. Nederland maakt hierin een eigenstandige afweging, op basis van factoren zoals deze ook bij het nemen van de voorzorgsmaatregel rondom Kaspersky antivirussoftware zijn gebruikt.

1) <https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/>

Minister van Justitie en Veiligheid

Datum
24 september 2018

Ons kenmerk
2355936

¹ Kamerstuk II 2017/18, 25 124, nr. 90