Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Vragen gesteld door de leden der Kamer

2019Z06368

Vragen van het lid **Bruins Slot** (CDA) aan de Minister en de Staatssecretaris van Defensie over *het tegengaan van ongewenste toegang tot het Netherlands Armed Forces Integrated Network (NAFIN)* (ingezonden 1 april 2019).

Vraag 1
Is het glasvezelnetwerk van Defensie, het Netherlands Armed Forces Integrated Network (NAFIN) van belang in het kader van de nationale veiligheid en dient dit zwaar beveiligd te zijn in het licht van de toenemende cyberdreiging?

Vraag 2
Deelt u de mening dat het van belang is om voorzieningen te treffen om het NAFIN te vrijwaren van ongewenste statelijke en non-statelijke beïnvloeding, spionage en sabotage?

Vraag 3
Hanteert u nog steeds het uitgangspunt dat over de middelen voor «command and control», waaronder de verbindingsstelsels, volledige beschikkingsmacht door Defensie vereist is en dat Defensie voor «command and control» niet afhankelijk van derden mag zijn?[1]

Vraag 4
Klopt het nog steeds dat het economisch eigendom van het NAFIN bij KPN ligt en dat u het eeuwig gebruiksrecht heeft?

Vraag 5
Klopt het dat in de afgelopen jaren steeds meer medegebruik door tweeden en derden plaatsvindt van het NAFIN, zoals de politie, C2000 (voor vaste verbindingen in het kernnetwerk), het civiele KPN Telecom satelliet-grondstation in Burum en de vier rijksoverheidsdatacenters (opvolger van alle 64 datacenters van het Rijk), die een groot deel van alle rijksoverheid informatie opslaat en ook de Rijkscloud bevat en de Haagse Ring?

[1] Kamerstuk 22 800 X, nr. 46

Vraag 6
Is de opsomming in vraag 5 van medegebruik door tweeden en derden volledig? Zo nee, welke organisaties of andere actoren missen in de opsomming?

Vraag 7
Klopt nog steeds het uitgangspunt voor medegebruik dat «Defensie onder alle omstandigheden de volledige zeggenschap over het NAFIN behoudt»?[2] Zo nee, op welke onderdelen en in welke situaties is daar geen sprake meer van?

Vraag 8
In hoeverre is er bij het medegebruik door tweeden en derden sprake van virtueel en/of gescheiden netwerken? Kunt u per medegebruiker aangeven of er sprake is van een virtueel gescheiden en/of fysiek gescheiden netwerk?

Vraag 9
In hoeverre is er op deze netwerken sprake van het verspreiden van gerubriceerde/geclassificeerde informatie? Kunt u een overzicht van welke gerubriceerde/geclassificeerde informatie over welke netwerken (NAFIN en de medegebruikers) verspreid kan/mag worden aan de Kamer toezenden? Klopt het nog steeds dat over het NAFIN tot en met geheim gerubriceerde e-mail kan worden verzonden?

Vraag 10
Herinnert u zich de verkenning door PWC naar gescheiden ICT-netwerken en -diensten in Nederland?[3] Bent u het met PWC eens, dat een deel van de kwetsbaarheid van ICT-netwerken zich bevinden in:
a. de oorsprong van de keten van ontwerp en bouw van het netwerk;
b. de upgrades van het netwerk: welke kwetsbaarheden zijn, al dan niet bewust, in componenten ingebouwd?
c. het beheer en het onderhoud van het netwerk: wie hebben toegang tot een netwerk via beheer en onderhoud en met welke intenties?[4]

Vraag 11
Op welke wijze hebt u rekening gehouden met deze ketenrisico's (zoals het mogelijk schenden van de vertrouwelijkheid van de inhoud van de communicatie) bij het NAFIN en de medegebruikers van het netwerk?

Vraag 12
Welk restrisico accepteert u voor NAFIN en het medegebruik? Wat is nodig om dit restrisico te mitigeren?

Vraag 13
Wie doet op dit moment of gaat in de toekomst het ontwerp, bouw, upgrades, beheer en onderhoud van het NAFIN en de medegebruikers zoals C2000, de Rijksdatacenters, de Haagse Ring, de Rijkscloud en overige medegebruikers doen? Kunt u een overzicht van NAFIN en per medegebruiker maken? In hoeverre is hier sprake van Nederlandse dan wel buitenlandse bedrijven?

Vraag 15
Hoe wordt voorkomen dat via ontwerp, bouw, upgrades, beheer en onderhoud van de medegebruikers van het NAFIN door buitenlandse bedrijven (bijvoorbeeld Chinese bedrijven) toegang wordt verkregen tot het militaire deel van het netwerk en dat daarmee de nationale veiligheid in gevaar kan komen? Kunt u de maatregelen apart benoemen voor de categorie ontwerp, bouw, upgrades, beheer en onderhoud?

---

[2] Kamerstuk 23 400 X, nr. 46
[3] Kamerstuk 26 643, nr. 337
[4] PWC, Verkenning naar gescheiden ICT-netwerken en -diensten in Nederland, september 2014

Vraag 16
Bent u bereid om, door middel van een risicoanalyse van het NAFIN en het medegebruik, de kans en impact van dreigingen in kaart te brengen om hier vervolgens mitigerende maatregelen aan te koppelen en over de kans en impact van dreigingen en de genomen en te nemen maatregelen de Tweede Kamer voor de zomer van 2019 te informeren? Zo nee, waarom niet?