Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

2565

Vragen van het lid **Eijsink** (PvdA) aan de minister van Defensie over *het bericht «Chinese hackers stelen ontwerp JSF en Patriot-raket»* (ingezonden 29 mei 2013).

Antwoord van minister **Hennis-Plasschaert** (Defensie) (ontvangen 14 juni 2013)

Vraag 1
Heeft u kennisgenomen van het bericht «Chinese hackers stelen ontwerp JSF en Patriot-raket»?[1]

Antwoord 1
Ja.

Vraag 2, 3, 4, 5, 6, 7 en 8
Welke gevolgen heeft het bekend zijn van het ontwerp en de technische gegevens voor de potentiële voorsprong die het JSF-toestel zou hebben op andere toestellen?
Welke gevolgen heeft het bekend zijn van het ontwerp en de technische gegevens voor het ontwikkelen van land- en luchtwapensystemen tegen de JSF?
Welke gevolgen heeft dit voor de potentiële veiligheid van het JSF-toestel?
Welke gevolgen kan het stelen van de ontwerp van de JSF hebben voor de ontwikkeling van de JSF?
Welke financiële gevolgen zijn te verwachten indien het ontwerp en de ontwikkeling van de JSF zullen worden aangepast als gevolg van het stelen van het huidige ontwerp van dit wapensysteem?
Kunt u aangeven welke maatregelen er zijn genomen door respectievelijk Lockheed Martin, het Pentagon en de Amerikaanse overheid als gevolg van het stelen van het ontwerp van de JSF?
Welke maatregelen gaat u nemen naar aanleiding van het stelen van het ontwerp van de JSF?

[1] http://www.nu.nl/algemeen/3485196/chinese-hackers-stelen-ontwerp-jsf-en-patriot-raket.html

ah-tk-20122013-2565
ISSN 0921 - 7398
's-Gravenhage 2013

Antwoord 2, 3, 4, 5, 6, 7 en 8
Het Amerikaanse ministerie van Defensie gaat om veiligheidsredenen niet in op berichten over mogelijke infiltraties van hun computersystemen. Dat geldt ook voor specifieke tegenmaatregelen. Wel is mij bekend dat vrijwel dagelijks, net zoals in andere landen, wordt getracht via het internet in computersystemen in te breken. Het Amerikaanse ministerie van Defensie neemt dergelijke pogingen zeer serieus en bestrijdt die intensief. Bij het ontwerp en de inrichting van computersystemen die vertrouwelijke informatie bevatten, wordt terdege rekening gehouden met de bescherming daarvan. Zo is hooggerubriceerde informatie niet opgeslagen op systemen die vanuit het internet toegankelijk zijn. Aangezien de data over de operationele capaciteiten van de F-35 hoog gerubriceerd zijn, is toegang tot deze informatie door digitale inbraak nagenoeg uitgesloten. De operationele veiligheid van de F-35 is niet in gevaar.
Zoals bekend neemt Defensie de beveiliging van vertrouwelijke informatie zeer serieus. De MIVD is voortdurend actief om (digitale) spionage tegen Defensie en met Defensie verbonden bedrijven te onderkennen en te verstoren. Hiertoe werkt de MIVD nauw samen met partnerdiensten in het buitenland. Dit geldt ook voor vertrouwelijke en hoog gerubriceerde informatie en de informatiesystemen waarop deze informatie is opgeslagen.
De berichtgeving in de media berust op een in de Verenigde Staten uitgevoerd onderzoek naar Cyber Security. Het openbare deel van het rapport *Resilient Military Systems and the Advanced Cyber Threat* over dit onderzoek bevat geen verwijzingen naar de F-35. In de Washington Post zijn op basis van gelekte informatie uit het niet-openbare deel van het rapport enkele wapensystemen gemeld waarbij in het verleden mogelijk sprake is geweest van hacking. Het betreft een veelvoud aan systemen en technologieën, waaronder de Patriot, F-35 en de F-18. Het rapport duidt niet op directe gevolgen voor het F-35 programma of voor het toestel.
Voor het F-35 programma is eerder gerapporteerd over een incident in 2007 waarnaar het artikel in de Washington Post ook verwijst. Zie ook de antwoorden van 22 april 2009 op vragen van het lid Brinkman (Kamerstuk 26 488, nr. 175) naar aanleiding van dit incident.