Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

2381

Vragen van de leden **Yesilgöz-Zegerius** en **Lodders** (beiden VVD) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Financiën over *het bericht «Vrees voor Chinese spionage via douanescanners in haven Rotterdam».* (ingezonden 3 februari 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), van Staatssecretaris **Van Huffelen** (Financiën – Toeslagen en Douane) (ontvangen 19 april 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 1778.

Vraag 1
Bent u bekend met het bericht «Vrees voor Chinese spionage via douanescanners in haven Rotterdam»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat bij de Nederlandse douane in de Rotterdamse haven, op vliegvelden en bij distributiecentra scanners worden gebruikt van het Chinese bedrijf Nuctech voor het controleren van goederen? Zo ja, voor welke taken worden deze scanners precies ingezet? Worden alle scanners als «stand-alone» gebruikt? Zo nee, hoeveel niet?

Antwoord 2
De Nederlandse Douane (hierna: de Douane) zet in de Rotterdamse haven, op de vliegvelden en bij distributiecentra scanners in, waaronder scanners van Nuctech. De scanners worden ingezet voor controle van goederen die de EU binnenkomen en uitgaan in o.a. containers, reizigersbagage, post- en koerierspakketten. Met de X-Ray scans wordt een scanbeeld gemaakt van de inhoud van containers. In de Rotterdamse haven zijn zeven grote ladingscanners geïnstalleerd, waaronder vier van Nuctech. Deze scanners zijn door middel van een gesloten glasvezel netwerk verbonden met het douanekan-

[1] fd.nl, 31 januari 2021, «Vrees voor Chinese spionage via douanescanners in haven Rotterdam», https://fd.nl/economie-politiek/1371071/zorgen-over-chinese-spionage-via-douanescanners-in-haven-rotterdam?utm_source=nieuwsbrief&utm_campaign=fd-ochtendnieuwsbrief_#126;SYSTEM.CAMPAIGNID#126;_#126;SYSTEM.MAILID#126;&utm_medium=email&utm_content=20210201&s_cid=671

ah-tk-20202021-2381
ISSN 0921 - 7398
's-Gravenhage 2021

toor Maasvlakte. Alle overige scanners in gebruik bij de Douane worden «standalone» gebruikt.

Vraag 3
Op welke Nederlandse vliegvelden en bij welke Nederlandse distributiecentra wordt gebruik gemaakt van Nuctech scanners? Zijn er nog andere Nederlandse instellingen/sectoren waar gebruik wordt gemaakt van Nuctech scanners? Zo ja, welke?

Antwoord 3
Nuctech maakt scanners voor uiteenlopende doeleinden. De overheid houdt geen totaaloverzicht bij van scanapparatuur die wordt gebruikt door de instellingen en sectoren.
Specifiek voor de Douane geldt dat de Douane Nuctech scanners inzet op de luchthavens Schiphol en Maastricht Aachen Airport voor vracht en reizigersbagage. Op Rotterdam The Hague Airport zet de Douane de scanners in voor reizigersbagage. Tevens zet de Douane scanners van Nuctech in bij distributiecentra, zoals de postsorteercentra.

Vraag 4
Is er een risico- en veiligheidsanalyse vooraf gegaan aan het besluit om de scanners van Nuctech aan te schaffen in onze mainports? Zo ja, is hierbij advies ingewonnen van (digitale) veiligheidsexperts over bijvoorbeeld het inbouwen van achterdeurtjes en het hanteren van een mogelijke *kill switch*? Zo nee, waarom niet?

Antwoord 4
De Douane besteedt structureel – onafhankelijk welke leverancier scan apparatuur levert – aandacht aan de bescherming en beveiliging van gegevens. Scan-apparatuur wordt door de Douane aangeschaft via wettelijk voorgeschreven inkoopprocedures op grond van de Aanbestedingswet. In een aanbesteding wordt getoetst of op een inschrijver de wettelijke uitsluitingsgronden uit de Aanbestedingswet van toepassing zijn.
Daarnaast maakt de Douane bij nieuwe aanbestedingen gebruik van het instrumentarium om risico's voor de nationale veiligheid bij inkoop en aanbesteding te adresseren. Dit instrumentarium is eind 2018 ontwikkeld ter ondersteuning van het ten aanzien van nationale veiligheidsrisico's verscherpt inkoop- en aanbestedingsbeleid voor de rijksoverheid. Bij de aanbesteding van de Nuctech scanners is het instrumentarium niet toegepast, omdat de quickscan op dat moment nog niet geïmplementeerd was. Bij toekomstige scan- en detectie aanbestedingen wordt het instrumentarium wel toegepast. Een nadere toelichting op dit beleid en instrumentarium wordt gegeven bij de beantwoording van vraag 5.
Tevens laat de Douane een externe audit uitvoeren op de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting, om te verzekeren dat de scan- en detectieprocessen zo veilig mogelijk zijn ingericht. De opdracht voor dit onderzoek is in september geïnitieerd nadat de Douane signalen ontving over de Nuctech scanners en het onderzoek zal in maart starten. Het doel van het onderzoek is om inzicht te verschaffen in het niveau van de informatiebeveiliging van de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting. Ook wil de Douane geïnformeerd worden over mogelijke risico's en advies over eventuele mitigerende maatregelen. Verwacht wordt dat de resultaten van het onderzoek in de zomer beschikbaar zijn. Daarnaast wordt in samenspraak met andere relevante overheidspartijen aanvullend onderzoek uitgevoerd, waarin de resultaten van deze externe audit worden meegenomen.

Vraag 5
Hoe beoordeelt u het grootschalige Nederlandse gebruik van Nuctech scanners in onze mainports met het oog op de constatering van onze inlichtingendiensten dat China een «offensief cyberprogramma heeft tegen Nederlandse belangen» en dat het daarom «onwenselijk is voor de uitwisse-

ling van gevoelige informatie/of vitale processen afhankelijk te zijn van IT-producten of diensten uit een land als China»?[2]

Antwoord 5
Zoals in het Dreigingsbeeld Statelijke Actoren (DBSA)[3] beschreven, is een toenemende afhankelijkheid van buitenlandse technologie een gegeven, aangezien geen land beschikt over alle kennis en productiemiddelen om technologisch onafhankelijk te opereren. Wel bestaat het risico dat met technologische toeleveringen de digitale spionage- en sabotagemogelijkheden toenemen.
Risico's voor de nationale veiligheid kunnen met name ontstaan wanneer deze technologie de Nederlandse vitale infrastructuur raakt, of wanneer deze technologie raakt aan gevoelige kennis en informatie. Een aanvullend risico kan ontstaan als er betrokkenheid is van leveranciers uit bepaalde landen die via nationale wet- en regelgeving gedwongen kunnen worden tot medewerking aan inlichtingenactiviteiten. De risico's voor de nationale veiligheid worden verder vergroot als het landen betreft die een offensief cyberprogramma voeren tegen de Nederlandse belangen en wanneer (technische) mogelijkheden om risico's te adresseren niet voorhanden zijn.
Om de weerbaarheid tegen deze dreiging te vergroten werkt de Minister van Justitie en Veiligheid samen met partners binnen en buiten de overheid aan de aanpak statelijke dreigingen, waarover uw Kamer op 3 februari j.l. de laatste stand van zaken heeft ontvangen[4]. Bij elke casus moet worden bezien hoe risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Uitgangspunt is dat maatregelen die hiertoe genomen worden proportioneel zijn. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiging en de (huidige) weerbaarheid.
Met betrekking tot het door uw Kamer genoemde vraagstuk is specifiek het overheidsbeleid dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten relevant. Bij de aanschaf van gevoelige apparatuur zal volgens dit beleid bij aanschaf en implementatie rekening gehouden worden met zowel eventuele risico's in relatie tot de leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Dit ten aanzien van nationale veiligheidsrisico's verscherpt inkoop en aanbestedingsbeleid is eind 2018 geïmplementeerd voor de rijksoverheid.
Ter ondersteuning van dit beleid is instrumentarium ontwikkeld dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen. De Douane past dit instrumentarium toe bij nieuwe aanbestedingen.

Vraag 6
Hoe beoordeelt u het besluit van Litouwen, Canada en de Verenigde Staten om de Nuctech scanners te weren vanwege het risico op spionage en misbruik van data door de Chinese overheid? Hoe beoordeelt u de constatering van de Amerikaanse Senaat dat Nuctech indirect is verbonden met het Chinese leger? Hoe beschouwt u bovenstaande in het licht van het Nederlandse gebruik van de Nuctech scanners en bijbehorende veiligheidsrisico's voor Nederland en in hoeverre bent u van mening dat aanschaf van Nuctech scanners nadere overweging verdient?

Antwoord 6
Het kabinet heeft aandacht voor ontwikkelingen in technologieën en kwetsbaarheden daarin. Ook de internationale (beleids)ontwikkelingen worden door het kabinet gevolgd.

---

[2] aivd.nl, «spionage en ongewenste inmenging», https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2018/spionage
[3] Kamerstuk 30 821, nr. 124
[4] Kamerstuk 30 821, nr. 125

Nederland maakt altijd een eigenstandige afweging. De Nederlandse overheid beziet de risico's die verbonden zijn aan producten en bedrijven op een zorgvuldige «case by case» basis.
Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij (digitale) producten hanteert het kabinet de overwegingen die zowel bij c2000[5] als bij de veiligheid van de telecomnetwerken[6] zijn gebruikt:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

3a. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?

3b. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

Deze overwegingen worden meegenomen is het in ons antwoord op vraag 4 genoemde aanvullende onderzoek, dat in samenspraak met andere relevante overheidspartijen wordt uitgevoerd.
In algemene zin kan worden gesteld dat de Chinese overheid nauw betrokken is bij het Chinese bedrijfsleven, zowel via staatsbedrijven als private bedrijven, en dat er sprake is van nauwe verwevenheid tussen civiele en militaire sectoren in China. Dit wordt ook beschreven in de beleidsnotitie «Nederland-China: een nieuwe balans»[7]. Over het kennisniveau van de Inlichtingen- en Veiligheidsdiensten worden in het openbaar geen uitspraken gedaan.

Vraag 7
Deelt u de mening dat het uit veiligheidsoogpunt zeer onwenselijk is dat een Chinees staatsgecontroleerd bedrijf nauw is betrokken bij strategische plekken in onze grensbewaking? Zo ja, bent u bereid om preventieve maatregelen te nemen die risico's op Chinese spionage beperken? Bent u bereid hiervoor onderzoek te laten doen naar het Nederlands gebruik van Nuctech scanners? Zo nee, waarom niet?

Antwoord 7
Zoals ook in de beantwoording van vraag 5 omschreven, bestaat het risico dat met technologische toeleveringen digitale spionage- en sabotagemogelijkheden toenemen.
Risico's voor de nationale veiligheid kunnen met name ontstaan wanneer deze technologie de Nederlandse vitale infrastructuur raakt, of wanneer deze technologie raakt aan gevoelige kennis en informatie. Een aanvullend risico kan ontstaan als er betrokkenheid is van leveranciers uit bepaalde landen die via nationale wet- en regelgeving gedwongen kunnen worden tot medewerking aan inlichtingenactiviteiten. De risico's voor de nationale veiligheid worden verder vergroot als het landen betreft die een offensief cyberprogramma voeren tegen de Nederlandse belangen en wanneer (technische) mogelijkheden om risico's te adresseren niet voorhanden zijn.
Bij elke casus moet worden bezien hoe eventuele risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Uitgangspunt is dat maatregelen die hiertoe genomen worden proportioneel zijn. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiging en de (huidige) weerbaarheid.

---

[5] Kamerstuk 25 124, nr. 96
[6] Staatsblad 2019, nr. 457
[7] Kamerstuk 35 207, nr. 1

Zoals ook vermeld bij de beantwoording van vraag 4, laat de Douane een externe audit uitvoeren op de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting, om te verzekeren dat de scan- en detectieprocessen zo veilig mogelijk zijn ingericht. De opdracht voor dit onderzoek is in september geïnitieerd nadat de Douane signalen ontving over de Nuctech scanners. Daarnaast wordt in samenspraak met andere relevante overheidspartijen aanvullend onderzoek uitgevoerd, waarin de resultaten van deze externe audit worden meegenomen.