Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

764

Vragen van de leden **Van Nispen** en **Leijten** (beiden SP) aan de Ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties over *Chinese drones die gebruikt worden door de politie* (ingezonden 1 oktober 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie (ontvangen 18 november 2021). Zie ook Aanhangsel Handelingen. Vergaderjaar 2021–2022, nr. 410.

Vraag 1
Klopt het dat de politie gebruikmaakt van drones van het Chinese merk Da Jiang Innovations? (DJI)[1]

Antwoord 1
Ja.

Vraag 2
Wat zijn de overwegingen geweest om te kiezen voor deze drones?

Antwoord 2
De politie heeft de drones aangeschaft via wettelijk voorgeschreven inkoopprocedures op grond van de Aanbestedingswet 2012. In een aanbesteding wordt getoetst of op een inschrijver de wettelijke uitsluitingsgronden van de Aanbestedingswet van toepassing zijn. De Aanbestedingswet 2012 biedt geen basis om producten van het bedrijf DJI uit te sluiten. Ook op de Nederlandse leverancier waren/zijn geen uitsluitingsgronden van toepassing. De Aanbestedingswet schrijft voor dat als er meerdere partijen zijn die voldoen aan de gestelde eisen, er moet worden gekozen voor de biedende partij met de beste prijs-kwaliteitverhouding.

Vraag 3
Klopt het dat het Ministerie van Defensie deze drones niet gebruikt, omdat ze deze te riskant vinden? Zo ja, wat zijn de overwegingen van Defensie?

[1] Website De Groene Amsterdammer, 30 september 2021 (https://www.groene.nl/artikel/made-for-china)

ah-tk-20212022-764
ISSN 0921 - 7398
's-Gravenhage 2021

Antwoord 3
Bij de aanschaf van een systeem beoordeelt Defensie de wijze waarop dit systeem zal worden ingezet. Indien daar vertrouwelijke en/of gerubriceerde informatie bij wordt vergaard geldt het Defensie Beveiligingsbeleid. Daarin is beschreven hoe deze informatie dient te worden behandeld. Dat betekent dat er beveiligingsmaatregelen worden geïmplementeerd om risico's te mitigeren. De zwaarte van deze maatregelen is gekoppeld aan het niveau van het te beschermen belang en de risico's in en rondom het systeem. Dat kan betekenen dat voor de behandeling van vertrouwelijke en/of gerubriceerde informatie bepaalde systemen niet mogen worden ingezet als de risico's te groot worden ingeschat.
In algemene zin kan worden gezegd dat Chinese dronefabrikanten een risico kunnen vormen omdat hun data op servers in China kunnen staan waarvan de beveiliging lastig is vast te stellen. De beheerders van die data kunnen bijvoorbeeld verplicht worden om data te leveren aan de overheid. Daarom is gebruik van dergelijke drones voor Defensie meestal niet mogelijk bij operationeel optreden. Dit sluit niet uit dat deze drones gebruikt worden voor andere doeleinden binnen Defensie, bijvoorbeeld voor het maken van luchtopnames van trainingen of evenementen. Voor operationele doeleinden beschikt Defensie over militaire drones die voldoen aan de gestelde beveiligingseisen.

Vraag 4
Klopt het dat de politie toegeeft dat er niet uitgesloten kan worden dat dronedata op Chinese servers belanden? Zo ja, waarom worden er dan alsnog extra van deze drones aangeschaft?

Antwoord 4
De politie heeft de berichten, die er vanaf het begin waren, waarin hiervan melding werd gemaakt niet kunnen verifiëren. De politie heeft hierop besloten de DJI-drones alleen in te zetten tijdens reguliere operaties. Dit zijn operaties waarbij geen vertrouwelijke informatie wordt verwerkt.

Vraag 5
Is er onderzoek gedaan door ICT-experts of de app die bij de drones hoort, toegang kan geven tot de telefoons van de agenten die hem gebruiken? Zo nee, waarom niet?

Antwoord 5
Een dergelijk onderzoek is niet aan de orde omdat de politie geen gebruik maakt van een app voor de bediening van DJI-drones. Voor de bediening van drones maakt de politie gebruikt de van zogeheten Smart Controllers van DJI. Deze Smart Controllers zijn stand-alone en bevatten de complete bediening inclusief een beeldscherm. Op deze Smart Controller staat de besturingssoftware om het toestel te besturen.

Vraag 6
Bent u bereid nader te onderzoeken of er politiedata gelekt zijn naar de Chinese fabrikant? Zo nee, waarom niet?

Antwoord 6
Ik zie, gezien de stappen die de politie al heeft gezet op dit gebied (zoals benoemd in antwoord 4 en 5), geen aanleiding om een nader onderzoek in te stellen. Er is tot op heden geen blijk geweest van een datalek. De politie is overigens verplicht ieder datalek direct te melden bij de Autoriteit Persoonsgegevens.

Vraag 7
Zijn er afspraken tussen de politie en DJI? Zo ja, kunnen die openbaar worden gemaakt?

Antwoord 7
De politie heeft alleen contact met DJI voor de instelling van het geofencingsysteem. Dit systeem zorgt ervoor dat de drones niet kunnen opstijgen in de zogenaamde no-fly zones (gebieden waar niet mag worden gevlogen met

drones). De politie heeft ontheffing voor veel no-fly zones. DJI heeft op verzoek van de politie deze instellingen aangepast.
Naar aanleiding van de Europese aanbesteding is er een raamovereenkomst gesloten met een Nederlandse leverancier die de DJI-drones conform deze overeenkomst levert aan de politie. In deze raamovereenkomst zijn de diverse (contract)afspraken vastgelegd, waaronder afspraken over data-security.

Vraag 8
Was u en/of de politie op de hoogte van de vele datalekken en onderzoeken rondom DJI? Zo nee, hoe kan dit?

Antwoord 8
De politie was op de hoogte van de berichten waarin werd gesproken over de mogelijkheid dat data weglekken naar Chinese servers. De politie heeft deze berichten echter niet kunnen verifiëren. Verder verwijs ik u naar het antwoord op vraag 4.

Vraag 9
Waarom vaart de politie op eigen expertise als het gaat om dataverzameling via externe leveranciers? Waarom is die expertise niet ingezet bij de technologie van kentekenscanners die ook aan gezichtsherkenning bleken te doen?

Antwoord 9
De politie besteedt structureel aandacht aan de bescherming en beveiliging van gegevens en veilige inkoop. Zo wordt een risico- en veiligheidsanalyse uitgevoerd door de informatiemanagement-functionaris en wordt indien van toepassing een gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd. Ook is in dit geval een security check uitgevoerd voor aanschaf van de drones.
Ten aanzien van het tweede deel van de vraag: de ANPR-camera's van de politie zijn niet uitgerust met gezichtsherkenningstechnologie.

Vraag 10
Kunt u een overzicht geven van welke overheidsinstanties nog meer gebruikmaken van technologie van dit bedrijf en voor wat voor werkzaamheden?

Antwoord 10
Een dergelijk overzicht is niet beschikbaar. Er is tot op heden geen aanleiding geweest om dat te inventariseren.

Vraag 11
Waarom zijn er geen Rijksbrede afspraken over het gebruik van technologie geproduceerd door bedrijven uit andere landen? Bent u bereid alsnog met Rijksbreed beleid hiervoor te komen? Zo nee, waarom niet?

Antwoord 11
Eind 2018 is instrumentarium ontwikkeld dat organisaties helpt bij het meewegen van nationale veiligheidsrisico's bij de inkoop- en aanbesteding van producten en diensten. Dit dient als hulpmiddel bij het uitvoeren van een risicoanalyse en het nemen van eventuele mitigerende maatregelen. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Op dit moment zie ik geen reden tot aanscherping van het staande beleid.

Vraag 12
Begrijpt u het advies van hoogleraar Oerlemans dat het nu de tijd is om goed na te denken over overheidsbevoegdheden op het gebied van cybersecurity en na te denken over wat hij checks and balances noemt? In hoeverre is dat al gebeurd in de afgelopen jaren, in integrale zin?[2]

Antwoord 12
Ja, dat is een begrijpelijk advies. Het nadenken over overheidsbevoegdheden en de «checks and balances» daaromtrent is een continu proces. In dit kader wijs ik graag op de Kamerbrief «Uitkomsten verkenning wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten» van 3 februari 2021.[3] Hierin wordt onder andere ingegaan op het Nederlandse cybersecuritystelsel en interventiemogelijkheden van de overheid in geval van digitale dreigingen en incidenten. Deze brief illustreert dat er binnen het kabinet continue aandacht is voor het vraagstuk rond overheidsbevoegdheden op gebied van cybersecurity. Dit is een proces dat nooit af is, en ik deel dan ook de visie van hoogleraar Oerlemans dat dit ook in het nieuwe kabinet continue aandacht vereist. Dit betreft overigens een ander vraagstuk dan het inkoopvraagstuk dat in de voorgaande vragen centraal staat.

Vraag 13
Denkt u dat als dit grondig was gedaan er niet met spoed een wetsvoorstel gemaakt moest worden voor de NCTV? Zo nee, waarom niet?

Antwoord 13
Het wetsvoorstel waar dhr. Oerlemans in het artikel aan refereert betreft het voorstel voor een Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid. Dit wetsvoorstel, dat op 9 november jl. aan uw Kamer is gestuurd, beoogt de juridische grondslag voor specifieke analyse- en coördinatiewerkzaamheden te verankeren die de NCTV namens de Minister van Justitie en Veiligheid uitvoert op het terrein van de nationale veiligheid en terrorismebestrijding en waarbij de verwerking van persoonsgegevens noodzakelijk wordt geacht. Ik heb daar in de brieven van 13 april 2021[4] en 21 mei 2021[5] uitvoerig aandacht aan besteed. Dit wetsvoorstel bevat geen specifieke overheidsbevoegdheden op het gebied van cybersecurity.

---

[2] Website De Groene Amsterdammer, 29 september 2021 (https://www.groene.nl/artikel/geheimhouding-of-openheid)
[3] Kamerstuk, vergaderjaar 2020–2021, 26 643, nr. 738
[4] Kamerstuk, vergaderjaar 2020–2021, 32 761, nr. 180
[5] Kamerstuk, vergaderjaar 2020–2021, 30 821, nr. 131