# 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**

## 765

Vragen van de leden **Michon-Derkzen**, **Brekelmans** en **Rajkowski** (allen VVD) aan de Ministers van Justitie en Veiligheid en van Buitenlandse Zaken over *het bericht «Hoe China met de Nederlandse politie meekijkt»* (ingezonden 1 oktober 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Ministers van Buitenlandse Zaken, Defensie en Infrastructuur en Waterstaat (ontvangen 18 november 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 409.

Vraag 1
Bent u bekend met het bericht «Hoe China met de Nederlandse politie meekijkt»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat de Nederlandse politie drones van het Chinese bedrijf Da Jiang Innovations (DJI) inzet? Zo ja, voor welke taken precies? Waarom is er gekozen voor drones van dit bedrijf?

Antwoord 2
Ja. De politie heeft bij de aanschaf van de drones, via een security check, een bewuste afweging gemaakt om de drones niet voor gevoelige operaties, maar alleen voor reguliere processen in te zetten. Dat wil zeggen: wel voor forensische opsporing, verkeersongevallenanalyse en openbare orde en veiligheid, maar niet operaties waarbij vertrouwelijke informatie wordt verwerkt.
De politie besteedt structureel aandacht aan de bescherming en beveiliging van gegevens en veilige inkoop. De drones zijn aangeschaft via wettelijk voorgeschreven inkoopprocedures op grond van de Aanbestedingswet 2012. De Aanbestedingswet 2012 biedt een aantal wettelijke gronden om een inschrijver uit te sluiten. Gezien het doel van de inzet van de drones was er geen reden om een beroep te doen op een van de uitsluitingsgronden. De

[1] Website Trouw, 30 september 2021 (https://www.trouw.nl/buitenland/hoe-china-met-de-nederlandse-politie-meekijkt~b3300703/)


ah-tk-20212022-765
ISSN 0921 - 7398
's-Gravenhage 2021

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
Is de aanschaf en het gebruik van drones van Da Jiang Innovations door de politie voorafgegaan door een risico- en veiligheidsanalyse? Zo ja, zijn daarbij (digitale) veiligheids- en privacyexperts geraadpleegd over het verzamelen van persoonsgegevens? Zo nee, waarom niet?

Antwoord 3
Zoals gezegd heeft de politie bij de aanschaf van de drones een security check uitgevoerd. Daarnaast is tijdens de projectfase een gegevensbeschermingseffectbeoordeling (GEB) gedaan. Uit deze beoordeling is niet gebleken dat er sprake is van verwerking van gegevens met een hoog risico. Er wordt alleen beeldmateriaal vastgelegd, dat versleuteld wordt verzonden. Niet kan worden uitgesloten dat deze beelden, ondanks de vastgelegde schriftelijke afspraken met de leverancier, toch bij DJI en/of Chinese overheid terecht komen, omdat DJI ook (naast de politie zelf) in het bezit is van de sleutel. Om deze reden heeft de politie mitigerende maatregelen genomen. Zo worden voor operaties waar vertrouwelijkheid gegevens worden verwerkt geen DJI-producten ingezet, maar andere vormen van luchtsteun.

Vraag 4
Klopt het dat de Nederlandse inlichtingendiensten hebben geconstateerd dat China een offensief cyberprogramma heeft tegen de Nederlandse nationale belangen? Hoe beoordeelt u het gebruik van drones van Da Jiang Innovations in dat licht? Deelt u de mening dat het onwenselijk is om voor politiewerk afhankelijk te zijn van Chinese hardware/IT-producten?

Antwoord 4
In openbare stukken zoals de jaarverslagen van de AIVD en de MIVD en het Dreigingsbeeld Statelijke Actoren (2021) geven de inlichtingen- en veiligheidsdiensten en de NCTV aan dat China één van de staten is waarvan is onderkend dat ze een offensief cyberprogramma hebben dat gericht is tegen Nederlandse belangen. De Chinese overheid gebruikt cyberoperaties om inlichtingen te verzamelen ter ondersteuning van haar economische, militaire en politieke doelstellingen.
In het algemeen geldt dat het afhangt van het inzetdoel of het gebruik van een bepaalde technologie veilig (genoeg) is en of eventuele risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Uitgangspunt is dat genomen maatregelen proportioneel zijn. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiging en de (huidige) weerbaarheid. De politie en Rijswaterstaat hebben beide een dergelijke analyse gemaakt voordat tot de aanschaf van de drones is over gegaan. Daarnaast is door de politie de afweging gemaakt de drones niet in te zetten voor processen waarbij het gaat om vertrouwelijke informatie.

Vraag 5
Klopt het dat Chinese bedrijven volgens de Chinese wet verplicht zijn om data af te staan aan hun overheid? Deelt u de mening dat het uit veiligheidsoogpunt zeer onwenselijk is dat er door de Nederlandse overheid IT-producten worden afgenomen bij een bedrijf dat data deelt met de Chinese overheid?

Antwoord 5
In algemene zin kan worden gesteld dat de Chinese overheid nauw betrokken is bij het Chinese bedrijfsleven, zowel via staatsbedrijven als private bedrijven. China kent daarnaast wetgeving die (buitenlandse) bedrijven dwingt om gegevens te delen met de overheid. Dit wordt ook beschreven in de beleidsnotitie «Nederland-China: een nieuwe balans».[2]

[2] Kamerstuk, 2018–2019, 35 207, nr. 1

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.
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 jl. 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.
Als hulpmiddel bij het uitvoeren van een dergelijke risicoanalyse en het nemen van eventuele mitigerende maatrelen is eind 2018 instrumentarium ontwikkeld dat organisaties helpt bij het meewegen van nationale veiligheidsrisico's bij de inkoop- en aanbesteding van producten en diensten. 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.
De DJI-drones die Rijkswaterstaat op dit moment gebruikt zijn in 2017 aangeschaft ten behoeve van een pilot. Het genoemde instrumentarium was toen nog niet beschikbaar. Voor de politie geldt dat toen de inkoop startte, dit instrumentarium nog niet was geïmplementeerd in de inkoopprocedures. Ook achteraf gezien – wanneer het genoemde instrumentarium wel zou zijn gebruikt – zou de uitkomst van het inkoopproces niet anders zijn geweest. Rijkswaterstaat en de politie verwerken immers geen vertrouwelijke gegevens met de DJI-drones.
Rijkswaterstaat en de politie maken voor de lopende en toekomstige aanbestedingen met een mogelijk risico voor de nationale veiligheid wel gebruik van het instrumentarium.

Vraag 6
Wordt er bij het inzetten van drones van Da Jiang Innovations door de politie gebruikgemaakt van eigen software of gebruikt de politie DJI-bedrijfssoftware? Bent u op de hoogte van de veiligheidsrisico's van het gebruik van DJI-software? Gebruikt de politie speciale overheidsdrones?

Antwoord 6
De politie gebruikt de besturingssoftware van DJI, maar er wordt geen gebruik gemaakt van de DJI-besturingsapp. De politie gebruikt geen speciale overheidsdrones. Voor het overige verwijs ik naar het antwoord op vragen 5 en 7.

Vraag 7
Bent u bereid om preventieve maatregelen te nemen die de risico's op Chinese spionage beperken? Bent u bereid hiervoor onderzoek te laten doen naar het gebruik door de politie van drones van Da Jiang Innovations? 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. Zoals gezegd is dit in het geval van de politie niet het geval. Een aanvullend risico kan ontstaan als er betrokkenheid is van leveranciers uit bepaalde landen die via nationale

[3] Kamerstuk, 2020–2021, 30 821, nr. 124
[4] Kamerstuk, 2020–2021, 30 821, nr. 125

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.
Ik zie, gezien de stappen die de politie al heeft gezet, geen aanleiding om een onderzoek in te stellen.

Vraag 8
Hoe beschouwt u het feit dat Defensie vanwege veiligheidsrisico's reeds geen gebruik meer maakt van DJI-drones? Hoe beschouwt u in dat licht het gebruik van DJI-producten door de politie?

Antwoord 8
Het hangt af van het inzetdoel of een bepaald type drone veilig (genoeg) is. Het uitgangspunt is dat eventuele risico's per casus in kaart moeten worden gebracht. Defensie heeft besloten om geen gebruik meer te maken van Chinese drones voor operationele taken, maar wel voor luchtopnames van trainingen of evenementen. Defensie heeft daarin haar eigen afweging gemaakt.
Bij de aanschaf van de drones heeft de politie, via een security check, een bewuste afweging gemaakt om drones niet voor gevoelige operaties, maar alleen voor reguliere processen in te zetten. Dat wil zeggen: wel voor forensische opsporing, verkeersongevallenanalyse en openbare orde en veiligheid, maar niet operaties waarbij vertrouwelijke informatie wordt verwerkt.

Vraag 9
Bent u bekend met het feit dat drones van DJI sinds 2020 niet meer gebruikt worden door de Verenigde Staten vanwege veiligheidszorgen en dat Japan dit overweegt? Hoe beoordeelt u dit? Heeft u hierover contact gehad met de VS en Japan? Zo nee, bent u bereid hierover contact op te nemen?

Antwoord 9
Nederland is eind 2020 door de VS geïnformeerd dat DJI op de entity list van het Bureau of Industrial Security van het Department of Commerce is geplaatst. In de publiekelijk beschikbare listing geven de VS aan dat zij DJI zien als een mogelijk risico voor de Amerikaanse buitenlandse politieke belangen.[5] Hierbij wijzen zij op de rol van o.a. DJI bij het mogelijk maken van mensenrechtenschendingen in China door hoogtechnologische surveillance en het exporteren van deze technologie naar derde landen waar repressieve regimes aan de macht zijn.
Japan verbiedt geen producten van specifieke landen of bedrijven maar heeft aanbestedingsrichtlijnen opgesteld voor gebruik van IT-producten door overheidsinstanties. Wanneer deze worden ingezet voor publieke veiligheid en orde, kritieke infrastructuur en het uitvoeren van reddingsacties, dient de Japanse overheid mogelijke risico's in kaart te brengen. Sinds april 2021 vallen drones ook binnen deze richtlijnen. Nadien zijn drones die als «hoog risico» worden aangemerkt zo snel mogelijk vervangen. Ook worden maatregelen getroffen om dataveiligheid van drones te garanderen.
Nederland ziet het gebruik van Chinese technologie niet als absoluut risico. Het inzetdoel van de technologie en de mogelijkheid om mitigerende maatregelen te treffen zijn bepalend of het verantwoord is om gebruik te maken van een bepaalde technologie.

[5] Federal Register: Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List.

Vraag 10
Is er binnen de NAVO of de EU gesproken over de veiligheid van het gebruik van deze drones? Gebruiken NAVO-bondgenoten en EU-lidstaten deze drones voor politie-, militaire of andere doeleinden?

Antwoord 10
Overwegingen rondom de veiligheid van het gebruik van dit type drones is een nationale aangelegenheid waarover in NAVO-verband niet wordt gesproken. Ook in EU-verband is niet gesproken over het gebruik van dit type drones. Het is het kabinet niet bekend welke andere NAVO-bondgenoten en EU-lidstaten deze drones gebruiken. NAVO zelf beschikt in ieder geval niet over dit type drones.

Vraag 11
Zijn er Europese landen die drones van een bedrijf uit een EU-lidstaat of OESO-land inzetten voor vergelijkbare taken als waar de Nederlandse politie de DJI-drones voor inzet? Zo ja, kunt u aangeven welke landen dit zijn en uit welke landen de bedrijven komen die ook drones in deze categorie produceren?

Antwoord 11
Het is het kabinet niet bekend welke drones er in andere Europese landen worden gebruikt.

Vraag 12
Hoe beoordeelt u het risico dat China de data van drones gebruikt voor het analyseren van Nederlandse (vitale) infrastructuur? Deelt u de inschatting van experts dat deze informatie zeer interessant is voor China?

Antwoord 12
Zoals gezegd worden de drones door de politie niet ingezet bij processen waarbij het gaat om vertrouwelijke informatie of vitale infrastructuur.
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 jl. de laatste stand van zaken heeft ontvangen.[6]
Zoals ook in mijn antwoord op vraag 4 gegeven moet bij elke casus 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.
Verder verwijs ik u graag naar het antwoord op vraag 7.

Vraag 13
Ziet u een gevaar van het gebruik van DJI-drones voor bijvoorbeeld Oeigoeren in Nederland, gezien het feit dat China gezichtsherkenningssoftware gebruikt om Oeigoeren te onderdrukken en ook de diaspora in Nederland onder druk zet?

Antwoord 13
Er zijn voor zover mij bekend momenteel geen aanwijzingen dat China de DJI-drones kan en zal gebruiken om bepaalde minderheidsgroepen in Nederland te monitoren. Mocht dit in de (nabije) toekomst wel het geval zijn, dan is er naar het oordeel van het kabinet sprake van ongewenste buitenlandse inmenging en heeft het kabinet verschillende instrumenten tot haar beschikking, zoals uiteengezet in de brief van 16 maart 2018 over de aanpak ongewenste buitenlandse inmenging.[7]
De politie kan tijdens demonstraties DJI-drones inzetten ten behoeve van de handhaving van de openbare orde en veiligheid. Tot op heden heeft de politie drones ingezet tijdens Coronaprotesten, Black Lives Matter-demonstraties, boerenprotesten en het Woonprotest in Rotterdam. In het kader van de mitigerende maatregelen rondom het gebruik van Chinese drones heeft de

[6] Kamerstuk, vergaderjaar 2020–2021, 30 821, nr. 125
[7] Kamerstuk, vergaderjaar 2017–2018, 26 643, nr. 42

korpsleiding van de politie besloten om bij bijvoorbeeld demonstraties voor de rechten van Oeigoeren andere luchtsteunmiddelen te gebruiken, bijvoorbeeld een helikopter of een militaire drone.

Vraag 14
Heeft u in algemene zin diplomatiek contact met China over de dataveiligheid van Chinese technologie voor Nederlandse gebruikers? Zo ja, wat is hierbij de Nederlandse inzet?

Antwoord 14
Ja, Nederland spreekt in verschillende verbanden, waaronder binnen de VN, met China over dataveiligheid. Centraal hierbij staat de bescherming van privacy, zoals de naleving van de Algemene Verordening Gegevensbescherming (AVG), bescherming van mensenrechten en het tegengaan van ongepaste toegang van overheden tot datagegevens. Zoals aangegeven in de notitie «Nederland-China: Een nieuwe balans» staat het kabinet achter striktere handhaving en sterker uitdragen van bestaande standaarden en normen, zoals de Europese regelgeving op het gebied van data, privacy en productveiligheid. Wat Nederland betreft dient China zich eveneens aan deze afspraken te conformeren.