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

3018

Vragen van de leden **Rajkowski**, **Brekelmans** en **Michon-Derkzen** (allen VVD) aan de Ministers van Justitie en Veiligheid en van Buitenlandse Zaken over *het bericht «Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries»* (ingezonden 9 maart 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), van Minister **Hoekstra** (Buitenlandse Zaken) en van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking (ontvangen 8 juni 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2273.

Vraag 1
Bent u bekend met het bericht «Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries»?[1]

Antwoord 1
Ja

Vraag 2
Klopt het dat het gaat om camera's van de Chinese merken Hikvision en Dahua en dat zij onder andere overheidsgebouwen in beeld brengen? Zo ja, om hoeveel camera's gaat het? Waar staan deze camera's? Staan deze camera's ook voor overheidsgebouwen waarbij anonimiteit belangrijk kan zijn zoals bij defensie en de inlichtingendiensten?

Antwoord 2
De Nederlandse overheid maakt gebruik van Chinese camera's. Het is niet bekend om hoeveel camera's het specifiek gaat. Zoals in het antwoord op vragen 4 en 5 wordt geschetst, gelden er overheidsbreed kaders en beleid voor aanschaf en gebruik van (digitale) producten en diensten, zoals camera's, waarbij ook rekening gehouden moet worden met (eventuele) risico's voor nationale veiligheid. Over welke beveiligingsmaatregelen al dan niet worden getroffen bij de gebouwen van de inlichtingen- en veiligheids-

[1] NOS, 8 februari 2022 (https://nos.nl/artikel/2416279-omstreden-chinese-camera-s-hangen-overal-in-nederland-ook-bij-ministeries).

ah-tk-20212022-3018
ISSN 0921 - 7398
's-Gravenhage 2022

diensten en welke apparatuur daarvoor wordt gebruikt, worden in het openbaar geen uitspraken gedaan.

Vraag 3
De politie heeft inmiddels bevestigd dat er vorig jaar bijna 700 camera's van Dahua zijn aangeschaft[2]; klopt dit? Zo ja, was de politie zich al bewust van de veiligheidsrisico's bij de aanschaf van deze camera's? Zo ja, waarom zijn dan toch deze camera's aangeschaft? Zo nee, kunt u een tijdlijn schetsen van de aanschaf van Chinese camera's door de politie van de afgelopen jaren? Zo nee, waarom niet?

Antwoord 3
De politie heeft bevestigd dat het klopt dat zij circa 700 camera's van Dahua heeft aangeschaft, die over een periode van 7 jaar zullen worden afgenomen. In de aanbesteding zijn eisen met betrekking tot informatiebeveiliging en privacy opgenomen en de inzet van de camera's zijn voornamelijk gericht op verkeerstoezicht. De politie heeft bij de aanbesteding van de camera's en bij de toepassing daarvan geen risico's voor de nationale veiligheid voorzien. Voor de gehele overheid geldt onder meer voor de aanschaf van digitale producten en diensten de Baseline Informatiebeveiliging Overheid (BIO). Mede gelet hierop worden hiervoor bij de inkoop en aanbesteding van digitale producten en diensten, waaronder genoemde camera's, waarbij mogelijk veiligheidsrisico's aan de orde zijn, eisen met betrekking tot informatiebeveiliging en privacy gesteld als voorwaarden aan de (mogelijke) opdrachtnemer. Alle merken en type camera's die voldoen aan de gestelde eisen kunnen worden aangekocht. Op 8 juli 2020 is deze aanbesteding gepubliceerd op Tenderned. Op 27 november 2020 is deze opdracht gegund. In mei 2021 is gestart met de ingebruikneming van deze camera's.

Vraag 4 en 5
In hoeverre lagen bepaalde productspecificaties zoals de prijs en de veiligheid ten grondslag aan het besluit om camera's van Hikvision en Dahua aan te schaffen en te plaatsen bij overheidsgebouwen?
Aan welke eisen, die betrekking hebben op cyberspionage, wordt getoetst bij de aanschaf van camera's bij overheidsgebouwen? Voldoen de camera's van Hikvision en Dahua aan deze eisen?

Antwoord 4 en 5
In relatie tot nationale veiligheidsrisico's bestaat er overheidsbeleid dat voorschrijft dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. Bij de aanschaf en implementatie van gevoelige apparatuur of programmatuur wordt volgens dit beleid rekening gehouden met zowel risico's in relatie tot een leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld als het gaat om de toegang tot systemen door derden. Bij elke casus wordt door de overheidsorganisatie bezien of en hoe risico's beheersbaar kunnen worden gemaakt en of daartoe te nemen maatregelen proportioneel zijn. Afwegingen rondom de aanschaf en ingebruikname van ICT- producten en diensten zijn de eigen verantwoordelijk van de organisaties die tot aanschaf overgaan. Dat betekent dat overheidsorganisaties zelf risicoafwegingen uitvoeren voordat (digitale) producten en diensten van een leverancier, zoals beveiligingscamera's, worden afgenomen en bepalen aan welke (beveiligings)eisen een leverancier moet voldoen om voor verlening van een opdracht in aanmerking te komen. Daarnaast geldt voor de gehele overheid voor de aanschaf van digitale producten en diensten de Baseline Informatiebeveiliging Overheid (BIO). De BIO kent een risicogebaseerde aanpak met een concrete set aan eisen als ondergrens. Uitgangspunt is onder meer ook de eigen verantwoordelijkheid van overheidsorganisaties.

[2] Nu.nl, 17 februari 2022 (https://www.nu.nl/tech/6184588/politie-kocht-bijna-zevenhonderd-omstreden-chinese-cameras.html?redirect=1)

Vraag 6
Was bij het moment van aankoop ook al bekend dat China eventueel een achterdeur in een camerasysteem van Hikvision of Dahua zou kunnen bouwen? Zo ja, welke maatregelen zijn hiertegen getroffen? Zo nee, op basis waarvan is de inschatting gemaakt dat het veilig was om deze camera's aan te schaffen?

Antwoord 6
Het Ministerie van BZK zal in samenwerking met andere overheidspartijen onderzoek doen naar mogelijke nationale veiligheidsrisico's bij het gebruik binnen de rijksoverheid van camera's afkomstig van partijen uit landen met een offensief cyberprogramma richting Nederland. Doordat het onderzoek zich specifiek richt op het gebruik van camera's binnen de rijksoverheid staat het los van de aanbesteding van de politie. De toepassing van de camera's en bijvoorbeeld de manier waarop zij in de bredere infrastructuur zijn ingebed zal per geval verschillen. Zoals ook in het antwoord op vraag 4 en 5 wordt geschetst, bestaat er overheidsbeleid dat voorschrijft dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. Of en hoe risico's voor de nationale veiligheid beheersbaar zijn, zal dus per geval worden beoordeeld door de organisaties zelf, zoals de politie, die ook eventuele maatregelen zelf nemen.

Vraag 7, 8 en 10
Is het technisch mogelijk voor China om mee te kijken, live of achteraf? Zo ja, hoe dan? Zo nee, is die mogelijkheid er helemaal niet of is hij sofwarematig dichtgezet?
Hoe groot acht de Minister de kans dat China meekijkt of mee heeft gekeken via deze camera's? Op basis waarvan maakt de Minister deze inschatting?
Deelt u de mening dat bedrijven uit staten die een offensief cyberprogramma tegen Nederland uitvoeren niet geschikt zijn om camera's te leveren die zijn opgesteld bij organisaties die een aantrekkelijk doelwit van een dergelijk offensief programma vormen?

Antwoord 7, 8 en 10
Het Dreigingsbeeld Statelijke Actoren (DBSA)[3] geeft een overzicht van de belangrijkste dreigingen vanuit China in relatie tot de vitale infrastructuur en de (rijks)overheid. Daarbij wordt ook ingegaan op het risico op digitale spionage- en sabotagemogelijkheden via technologische toeleveringen.
Zoals gesteld in het antwoord op vraag 6 zal het Ministerie van BZK in samenwerking met andere overheidspartijen onderzoek doen naar mogelijke nationale veiligheidsrisico's vanwege het gebruik binnen de rijksoverheid van camera's afkomstig van partijen uit landen met een offensief cyberprogramma richting Nederland. Bovenstaande vragen zullen bij dit onderzoek worden betrokken.
In het debat met uw Kamer op 22 maart 2022, heeft de Staatssecretaris voor Koninkrijksrelaties en Digitalisering verder toegezegd om onderzoek te doen naar inkoopeisen en -richtlijnen op het terrein van cyberveiligheid, in het bijzonder als het gaat om producten en diensten voornamelijk van partijen uit landen met een offensief cyberprogramma richting Nederland. Op 5 april 2022 is in aanvulling daarop door uw Kamer een motie aangenomen om bij dit onderzoek ook te kijken naar de vitale infrastructuur. Uw Kamer zal hierover na afronding van het onderzoek worden geïnformeerd. Op de uitkomsten van het onderzoek kan nu niet vooruit worden gelopen.

Vraag 9
In de Verenigde Staten is de inzet van Hikvision- en Dahua-camera's bij overheidsgebouwen verboden. Daarnaast heeft het Europees Parlement eerder besloten om camera's van Hikvision niet meer te gebruiken. Waarom heeft Nederland hier nog niet voor gekozen?

[3] Kamerstuk 30 821, nr. 124

Antwoord 9
Elk land of internationale organisatie maakt hierin zijn eigen afweging. Voor Nederland geldt dat het staand beleid bij inkoop en aanbesteding is dat er per casus wordt bezien of er in relatie tot producten en diensten risico's zijn voor de nationale veiligheid, en zo ja, of en hoe deze beheersbaar kunnen worden gemaakt. De mogelijke nationale veiligheidsrisico's in verband met het gebruik van camera's, die afkomstig zijn uit landen met een offensief cyberprogramma richting Nederland, binnen de rijksoverheid zullen, zoals hierboven aangegeven, worden onderzocht.

Vraag 11
Zijn er Europese alternatieven in de markt? Zo, ja bent u het eens met het standpunt dat het verstandig kan zijn om die in te zetten? Zo nee, bent u het ermee eens dat het wenselijk is dat er Europese alternatieven zijn, ook op het gebied van technologie?

Antwoord 11
Voor Nederlandse organisaties is het wenselijk dat zij gebruik kunnen maken van kwalitatief hoogwaardige producten en diensten, ook van buitenlandse leveranciers. Nederlandse overheden blijven op verantwoorde wijze, met inachtneming van de nationale aanbestedingswetgeving, gebruik maken van de voordelen van de internationale markt voor veiligheidsapparatuur, door per situatie de risico's voor de nationale veiligheid in kaart te brengen en dat te laten meewegen in de selectie van de betreffende aanbieder.
Desondanks kunnen er redenen zijn om bepaalde producten en technologieën in Nederland of in Europa te willen kunnen ontwikkelen en beschikbaar maken. Dit kan van belang zijn om de weerbaarheid van Nederland en de EU te vergroten, of om de EU het vereiste handelingsvermogen te geven om de eigen veiligheidsbelangen te beschermen. Dit kan via verschillende maatregelen: van handelsverdragen met gelijkgezinde landen, tot het direct stimuleren van de eigen industrie. Hierbij verwijzen wij dan ook graag naar de brief aan uw Kamer over onderzoek naar strategische afhankelijkheden en kwetsbaarheden in Nederland, waar dieper ingegaan wordt op de beleidsopties om onze weerbaarheid te versterken.[4]

Vraag 12
Bent u het ermee eens dat we de cyberdreiging vanuit China serieus moeten nemen en daarom kritisch moeten kijken naar de aanschaf en inzet van niet Europese hardware en software voor gevoelige zaken zoals het filmen van overheidsgebouwen? Zo ja, welke stappen gaat u ondernemen? Zo nee, waarom niet?

Antwoord 12
Ja, deze dreiging moet serieus worden genomen. De AIVD waarschuwt regelmatig voor de risico's van het gebruik van hard- en software afkomstig uit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen (zoals China) bij de uitwisseling van gevoelige informatie of in vitale infrastructuur. Het is van groot belang dat we ongewenste activiteiten van statelijke actoren tegengaan. Daarom werken we aan een aanpak om de weerbaarheid tegen statelijke dreigingen te verhogen. In het Dreigingsbeeld Statelijke Actoren en de kabinetsreactie hierop wordt nader ingegaan op deze dreiging en de maatregelen die we hiertegen nemen[5]. Verder verwijzen wij u naar het antwoord op vraag 4 en 5, waarin wordt ingegaan op de relevante kaders en beleid binnen de rijksoverheid als het gaat om aanschaf en gebruik van (digitale) producten en diensten.

Vraag 13
Hoe verhoudt het antwoord op de Kamervragen van het lid van Helvert (Aanhangsel Handelingen II, vergaderjaar 2020–2021, nr 2310), die de Kamer zijn toegezonden op 13 april 2021 (waarin staat dat het kabinet de Europese Commissie, de Europese Dienst voor Extern Optreden (EDEO) en het Europees Parlement heeft gewezen op de kwetsbaarheid van het gebruik van

[4] Kamerstuk 35 570, nr. 26
[5] Kamerstuk 30 821, nr. 125

Hikvision-camera's) zich tot het gebruik van camera's van dit bedrijf door Nederlandse ministeries zelf? Zou het kabinet deze waarschuwing niet ook aan zichzelf moeten richten?

Antwoord 13
In hoeverre er bij het gebruik van camera's van bijvoorbeeld Hikvision en Dahua sprake is van nationale veiligheidsrisico's die met concrete beheersmaatregelen gemitigeerd kunnen worden is onderwerp van het in het antwoord op vraag 6 genoemde onderzoek.

Vraag 14
Kunt u uitsluiten dat deze camera's een veiligheidsdreiging vormen voor de Oeigoerse diaspora in Nederland? Welke veiligheidsmaatregelen heeft u hiertoe genomen of bent u voornemens te nemen?

Antwoord 14
Zoals aangegeven in de antwoorden op vragen van de leden Dekker-Abdulaziz en Van Ginneken, zijn voor zover ons bekend er momenteel geen aanwijzingen dat China deze camera's gebruikt 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[6].

Vraag 15
Bent u bekend met het feit dat de Amerikaanse overheid heeft verboden te investeren in Hikvision vanwege de banden van het bedrijf met het Chinese leger? Heeft u hierover contact gehad met Amerika, met name in het kader van mogelijke veiligheidsdreigingen? Zo nee, bent u alsnog bereid dit te doen?

Antwoord 15
Het kabinet is bekend met het besluit van 9 oktober 2019 om Hikvision op de zgn. *Entity List* te plaatsen omdat Hikvision volgens de VS het mogelijk maakt dat er mensenrechtenschendingen plaatsvinden in Xinjiang. Als gevolg van deze *listing* zijn Amerikaanse toeleveranciers verplicht om vergunningen aan te vragen voordat ze handelen met Hikvision. Europese en Nederlandse sanctiewetgeving voorzien niet in de mogelijkheid van een *Entity List*. Nederland erkent de risico's van het gebruik van cybersurveillance items in relatie tot schendingen van mensenrechten en het internationaal humanitair recht, blijkens ons exportcontrolebeleid, en werkt hierop nauw samen met de VS, zowel bilateraal als in EU-verband.

Vraag 16
Bent u bereid om met China in gesprek te treden over het belang van privacy- en veiligheidsstandaarden in technologie en dat toegang van de Chinese staat tot gevoelige data niet acceptabel is?

Antwoord 16
Nederland en de EU spreken in verschillende verbanden, waaronder binnen de VN, met China over dataveiligheid. Centraal hierbij staat de bescherming van privacy, zoals het voldoen aan eisen, zoals neergelegd in de AVG, bescherming van mensenrechten en het tegengaan van ongepaste toegang van overheden tot datagegevens. Zoals aangegeven in de Notitie «Nederland-China: Een nieuwe balans» (Kamerstuk 35 207, nr. 1) staat het kabinet achter striktere handhaving en sterker uitdragen van bestaande standaarden en normen, zoals de Europese regelgeving op het gebied van data, bescherming van persoonsgegevens en privacy en productveiligheid.

[6] Kamerstuk 30 821, nr. 26 643, nr. 42