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

3019

Vragen van de leden **Dekker-Abdulaziz** en **Van Ginneken** (beiden D66) aan de Ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties over *het gebruik van omstreden Chinese bewakingscamera's door de Nederlandse overheid en politie* (ingezonden 10 maart 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) en van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Buitenlandse Zaken (ontvangen 8 juni 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2295.

Vraag 1
Hoe beoordeelt u dit bericht? Kunt u het gebruik van omstreden Chinese bewakingscamera's door de Nederlandse overheid ofwel de Nederlandse politie bevestigen?[1]

Antwoord 1
Ja, de Nederlandse overheid maakt gebruik van Chinese camera's.

Vraag 2
Kunt u verder uitweiden over de mogelijke veiligheidsrisico's die deze bewakingscamera's met zich mee brengen?

Antwoord 2
Het gebruik van digitale producten en diensten kan nationale veiligheidsrisico's met zich meebrengen. Gelet daarop heeft de overheid onder meer beleid ontwikkeld dat voorschrijft dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. De relevante kaders en beleid zijn in het antwoord op vraag 3 geschetst. 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. Indien dit onderzoek is afgerond zal uw Kamer daarover worden geïnformeerd. Specifiek voor de

[1] Follow the Money, 8 februari 2022 (https://www.ftm.nl/artikelen/de-ogen-van-chinees-staatsbedrijf-hikvision-zijn-overal?share=2MLXgQDtzdJhx8GyErjYy1NMmfs5uw1Qo0%2BOtO8emIxRKemeXHp2PQmmTh4vboE%3D)

ah-tk-20212022-3019
ISSN 0921 - 7398
's-Gravenhage 2022

politie geldt dat de aangeschafte camera's voldoen aan de gestelde eisen voor informatiebeveiliging en privacy en dat de camera's voornamelijk zijn gericht op verkeerstoezicht. Het huidige overheidsbeleid voor inkoop en aanbesteding volgend heeft de politie zelfstandig een afweging gemaakt met betrekking tot het afnemen van deze camera's. De politie heeft bij de aanbesteding van de camera's en bij de toepassing daarvan geen risico's voor de nationale veiligheid voorzien.

Vraag 3
Is bij de afweging voor aanschaf van deze bewakingscamera's het risico op misbruik van het camerasysteem door statelijke actoren een expliciet toetsingscriterium geweest en hoe is dat risico destijds beoordeeld?

Antwoord 3
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[2].

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. Daarom is er geen centraal overzicht beschikbaar van Chinese camera's in gebruik bij de overheid en eventuele risico's die daarmee verbonden zijn en ook niet van de afwegingen die ten grondslag lagen bij de aankoop.
Tevens is er ook expliciet aandacht voor de bescherming van persoonsgegevens, die worden verwerkt bij het gebruik van beveiligingscamera's. Deze verwerking van persoonsgegevens dient te voldoen aan de wettelijke eisen die daaraan zijn gesteld. De Algemene Verordening Gegevensbescherming bevat de regeling hiervan. Met een data protection impact assessment (DPIA) wordt in kaart gebracht of er een goede grondslag is voor de verwerking is en of de verwerking noodzakelijk en proportioneel is. Indien er in dat verband risico's gesignaleerd worden, wordt in kaart gebracht welke maatregelen genomen worden om die risico's aan te pakken.

Vraag 4
Kunt u een update geven over de huidige risico's die we momenteel lopen wat betreft Chinese invloed binnen de Nederlandse overheidssystemen zowel binnen de rijksoverheid als binnen de politie? Kunt u daarbij ingaan op de veiligheidsrisico's die er momenteel spelen bij het gebruik van deze systemen en specifiek ingaan op de situatie omtrent bewakingscamera's?

[2] Zie bijvoorbeeld het Jaarverslag AIVD 2019 p. 9.

Antwoord 4
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 hierboven aangegeven is er in lijn met deze aanpak overheidsbeleid dat voorschrijft dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. Opdrachtgevers zijn zelf verantwoordelijk voor de toepassing van dit beleid, de overheid heeft geen overzicht van Chinese apparatuur en programmatuur in gebruik bij de overheid.
In de beleidsreactie op het DBSA wordt aangegeven op welke manier het kabinet met de dreiging van statelijke actoren omgaat[4]. 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 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. Voor wat betreft camera's zal, zoals aangegeven in het antwoord op vraag 2, het Ministerie van BZK in samenwerking met andere relevante overheidspartijen onderzoek doen naar mogelijke nationale veiligheidsrisico's door het gebruik van camera's binnen de rijksoverheid afkomstig uit landen met een offensief cyberprogramma richting Nederland.

Vraag 5
De VS verwijderde de Hikvision en Dahua apparatuur al in 2019 bij federale overheidsgebouwen. Heeft de Nederlandse overheid naar aanleiding van dit besluit in de VS onderzoek gedaan naar de risico's bij het gebruik van dit soort camera's en andere gevoelige systemen bij Nederlandse overheidsdiensten? Zo nee, wat zijn de overwegingen hierachter geweest? Wat is er in het verleden verder gedaan om dit soort risico's te voorkomen?

Antwoord 5
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 6
Bent u bekend met de motie Buitenweg en Verhoeven (30 821-90) uit 2019 over onderzoek naar surveillanceapparatuur van Chinese bedrijven waar geen vervolg aan is gegeven?

Antwoord 6
Daar zijn wij mee bekend. De ingediende motie van Buitenweg en Verhoeven bij het VAO Nationale Veiligheid van 25 juni 2019 is aangehouden tijdens de stemmingen van 2 juli 2019, omdat de geuite zorgpunten in een eerder toegezegde brief (in het AO Nationale Veiligheid en Crisisbeheersing van 20 juni 2019) zouden worden meegenomen. In dit AO Nationale Veiligheid en Crisisbeheersing heeft de ambtsvoorganger van de Minister van Justitie en Veiligheid toegezegd een brief te sturen over het gebruik van technologieën als gezichtsherkenningssoftware voor de opsporing en de daarmee gepaarde risico's. Met de brief van 20 november 2019 (Kamerstuk 32 761 en 30 821, Nr. 152) is aan die eerdere toezegging gestand gedaan.
Direct nadat de brief naar uw Kamer is gestuurd is de politie gestart met de ontwikkeling van een inzetkader voor het gebruik van gezichtsherkennings-

[3] Kamerstuk 30 821, nr. 124
[4] Kamerstuk 20 821, nr. 125

technologie door de politie. Met behulp van dit inzetkader kunnen plannen voor het gebruik van gezichtsherkenningstechnologie juridisch en ethisch worden getoetst. Dit inzetkader zal naar verwachting nog voor de zomer van 2022 definitief worden vastgesteld, waarna het gebruik ervan binnen de politie verplicht zal zijn. Dit kader zal zowel inhoudelijke beoordelingsdimensies bevatten als de procedures die (verplicht) moeten worden gevolgd om te zorgen dat deze correct en zorgvuldig zijn toegepast.

Vraag 7
Hoe staat u momenteel tegenover een dergelijk onderzoek?

Antwoord 7
Aanvullend onderzoek naast het hierboven aangekondigde onderzoek en bestaande trajecten zoals het inzetkader voor gezichtsherkenning wordt op dit moment niet nodig geacht. Het staande kabinetsbeleid is dat overheidsorganisaties primair zelf verantwoordelijk zijn voor het meenemen van nationale veiligheidsoverwegingen in de inkoop en aanbesteding van producten en diensten.

Vraag 8
Bent u het ermee eens dat de rijksoverheid moet stoppen met gebruik van dit soort systemen op gevoelige plekken bij de rijksoverheid of bij de politie?

Antwoord 8
Zoals ook in het DBSA wordt benoemd en in antwoord op vraag 4 wordt gesteld, zitten aan de inzet van camera's ook risico's verbonden. Het is van belang dat de nationale veiligheidsrisico's worden meegewogen bij de inkoop en het gebruik hiervan. De relevante kaders en beleid hiertoe, zoals geschetst in het antwoord op vraag 3, houden in dat er per situatie een beoordeling plaatsvindt of er in relatie tot de aanschaf van een product of dienst sprake is van (eventuele) risico's voor nationale veiligheid en of die risico's voldoende beheersbaar kunnen worden gemaakt.

Vraag 9
Bent u verder bekend met het feit dat Hikvision en Dahua mogelijk worden ingezet door de Chinese overheid om Oeigoeren en andere minderheidsgroepen te onderdrukken? Hoe oordeelt u over deze associatie tussen beide bedrijven en grove mensenrechtenschendingen?

Antwoord 9
Er zijn rapporten verschenen die Hikvision en Dahua linken aan de surveillance van Oeigoeren en andere minderheden in Xinjiang[5].
Daarnaast is het kabinet bekend met rapporten en getuigenissen over grove mensenrechtenschendingen in Xinjiang. Met behulp van het gebruik van big data en camera's met gezichtsherkenning vergroten Chinese autoriteiten de controle over de bevolking.
Het kabinet maakt zich ernstige zorgen over de mensenrechtensituatie in China, waaronder de vergaande surveillance. Het kabinet stelt deze zorgen consequent aan de orde in verschillende gremia, zowel bilateraal als in EU- en VN-verband.

Vraag 10
Kunt u een update geven over de veiligheidsrisico's die de Oeigoerse diaspora in Nederland loopt door dit soort systemen te gebruiken? Hoe denkt het kabinet de veiligheidssituatie van deze groep en andere kwetsbare diaspora groepen te verbeteren? Kunt u daarbij specifiek ingaan op de overheidssystemen die hierbij mogelijk een kwetsbare rol in spelen?

[5] Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond (parliament.uk), Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang (ipvm.com).

Antwoord 10
Er zijn voor zover het kabinet bekend 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 11
Klopt het dat 10 gemeenten hebben besloten de camera's van Chinese fabrikanten te verwijderen? Zo ja, welke gemeentes waren dit en wat waren hun afzonderlijke precieze overwegingen om deze beslissing te nemen? Welke lessen trekt het kabinet hier uit voor de Nederlandse overheidsdiensten en de politie?

Antwoord 11
De VNG heeft geen inzicht in de afwegingen van individuele gemeenten over de inzet van technologie. De VNG werkt samen met gemeenten aan oplossingen om de inkoop en inzet van camera's transparanter, verantwoorder en veiliger te maken, ook in relatie tot het mensenrechtenbeleid van landen of bedrijven. Gemeenten hebben in 2019 een set algemene Principes voor de Digitale Samenleving vastgesteld en inkoopvoorwaarden gemaakt voor innovatieve technologie, welke zij in 2022 uitbreiden en actualiseren voor de inzet van technologie voor crowd-monitoring, zoals camera's. Op het gebied van veiligheid ondersteunt de VNG gemeenten al bij de afweging en inkoop van dit soort technologie met de Gemeentelijke Inkoop bij IT Toolbox-GIBIT en de integrale risico- en privacy-analyse (IRPA).
De politie zal voor taakuitvoering op grond van artikel 3 Politiewet en/of 126 Wetboek van Strafvordering[7] voor nu gebruik blijven maken van camerasystemen van Dahua, op basis van de overwegingen als aangegeven bij vraag 2. Bij vraag 2 is daarnaast aangegeven dat het Ministerie van BZK in samenwerking met andere relevante overheidspartijen onderzoek zal doen naar mogelijke nationale veiligheidsrisico's door het gebruik van camera's binnen de rijksoverheid afkomstig uit landen met een offensief cyberprogramma richting Nederland.
Naar aanleiding van de berichtgeving over Chinese camera's heeft de Vereniging Nederlandse Gemeenten (VNG) onderstreept dat gemeenten ethiek en publieke waarden centraal stellen bij de inzet van technologie. De VNG werkt al samen met gemeenten aan oplossingen om de inkoop en inzet van camera's transparanter, verantwoorder en veiliger te maken. Recente berichten over camera's van Chinese leveranciers onderstrepen de urgentie ervan.

Vraag 12
Bestaan er landelijke richtlijnen bij het gebruiken van dit soort risicovolle systemen voor gemeenten als bedrijven? Zo nee, acht u dat nodig?

Antwoord 12
Er is een instrumentarium ontwikkeld dat overheidsorganisaties helpt bij het meewegen van nationale veiligheidsrisico's bij de inkoop en aanbesteding van producten en diensten. De Informatiebeveiligingsdienst (IBD) van de VNG adviseert daarnaast gemeenten bij de inzet van technologie ook ten aanzien van spionage. In het kader daarvan leggen gemeenten aanvullend de nadruk op drie aandachtspunten:
Actieve versterking van het bewustzijn (onder bestuurders, managers en medewerkers) met betrekking tot de waarde van de informatie waarover zij beschikken en van de mogelijke interesse van criminelen en buitenlandse overheden.
Werken aan een veilige cultuur. Daarbij zijn gebruikers, de inrichting van gegevensstromen en databases en de gebruikte technieken voor detectie van incidenten belangrijke aandachtspunten.

---

[6] Kamerstuk 30 821, 26 643, nr. 42
[7] https://www.politie.nl/informatie/over-het-gebruik-van-anpr-fotos.html

Ondersteuning vanuit de fabrikant van een product door middel van software-updates vanuit de fabrikant. Na menselijke fouten ontstaan de meeste incidenten door misbruik van ongepatchte kwetsbaarheden in soft- en hardware. Het up-to-date houden van soft- en hardware verkleint niet alleen het risico op incidenten maar ook het risico op spionage door staten en criminelen.

Vraag 13
Kunt u verder uitweiden welke maatregelen er momenteel nog meer worden genomen om Chinese spionage bij de Nederlandse overheidsdiensten en de politie te voorkomen?

Antwoord 13
Zoals in het antwoord op vraag 4 wordt beschreven word in het Dreigingsbeeld Statelijke Actoren en de betreffende kabinetsreactie ingegaan op de dreiging die uitgaat van statelijke actoren, waaronder spionage door China, en de maatregelen die hiertegen worden genomen[8]. Daarnaast is op 28 februari jl. het wetsvoorstel uitbreiding strafbaarheid spionage in consultatie gegaan die een nieuwe bepaling aan het Wetboek van Strafrecht toevoegt. Op grond van die bepaling wordt het verrichten van handelingen ten behoeve van een buitenlandse mogendheid strafbaar indien daardoor zwaarwegende Nederlandse belangen worden geschaad. Omdat spionageactiviteiten steeds vaker digitaal plaatsvinden, wordt met het wetsvoorstel eveneens de strafmaat van een aantal computerdelicten verhoogd wanneer deze zijn gepleegd ten behoeve van een buitenlandse mogendheid.

Vraag 14
Kunt u tot slot uitleggen wat er naar aanleiding van dit bericht concreet gaat gebeuren? Kan de Minister daarbij ingaan op waarom de Nederlandse rijksoverheid ofwel politie wel of niet gebruik zal maken van Chinese beveiligingssystemen en daarbij specifiek ingaan op de systemen van Hikvision en Dahua?

Antwoord 14
De relevante kaders en beleid, zoals geschetst in het antwoord op vraag 3, blijven van toepassing. Op basis daarvan zal binnen de overheid per situatie gekeken worden of en hoe eventuele risico's voor de nationale veiligheid die verbonden zijn aan een product beheersbaar kunnen worden gemaakt. Zoals vermeld zal BZK in samenwerking met andere overheidspartijen onderzoek doen naar mogelijke nationale veiligheidsrisico's bij het gebruik van dergelijke camera's binnen de rijksoverheid. De politie zal, zoals vermeld in vraag 11, camera's van Dahua blijven gebruiken.

Vraag 15
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord 15
Ja.

[8] Kamerstuk 30 821, nr. 125