Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

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

3922

Vragen van het lid **Sjoerdsma** (D66) aan de Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking over *het bericht «Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest»* (ingezonden 18 juli 2019).

Antwoord van Minister **Kaag** (Buitenlandse Handel en Ontwikkelingssamenwerking), mede namens de Minister van Buitenlandse Zaken (ontvangen 10 september 2019).

Vraag 1
Bent u bekend met het bericht «Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat twee Nederlandse technologiebedrijven emotieherkenningssoftware hebben geleverd aan de Chinese staat? Klopt het dat deze bedrijven deze software hebben geleverd aan het Chinese Ministerie van Openbare Veiligheid en aan de Chinese politieacademie? Kunt u toelichten vanaf wanneer deze bedrijven aan de Chinese staat emotieherkenningssoftware leveren?

Antwoord 2
Het bedrijf stelt in het bericht dat er een levering heeft plaatsgevonden van het product aan het Chinese Ministerie van Openbare Veiligheid. Het product is, aldus Noldus, een samenwerking van de bedrijven Noldus en Vicar Vision – het gaat om één gezamenlijke levering van de twee bedrijven. Het bedrijf geeft aan dat de software geschikt is voor het herkennen van emoties op individuele gezichten – en niet identiteit – en daarmee is deze volgens Noldus niet geschikt voor surveillance.

[1] https://decorrespondent.nl/10307/berucht-chinees-veiligheidsministerie-gebruikt-nederlandse-software-die-emoties-leest/317002092-cae75d58

ah-tk-20182019-3922
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 3
Klopt het dat het Chinese Ministerie van Openbare Veiligheid verantwoordelijk is voor hightech surveillance die leidt tot privacyschendingen van Chinese burgers? En klopt het ook dat ditzelfde ministerie ook verantwoordelijk is voor de ernstige onderdrukking van de Oeigoeren in Xinjiang?

Antwoord 3
Er zijn verschillende Chinese overheidspartijen betrokken bij de (digitale) surveillancesystemen die in het land zijn opgetuigd. Vast staat dat het Ministerie van Openbare Veiligheid één van die partijen is. Ook bij de surveillance, de veiligheidsmaatregelen en de internering van moslimminderheden in heropvoedingscentra in Xinjiang speelt het ministerie – en de provinciale afdeling voor openbare veiligheid – waarschijnlijk een rol.

Vraag 4, 5
Bent u bekend met de plannen van de Chinese staat om in 2020 alle naar schatting 200 miljoen openbare beveiligingscamera's te integreren tot één groot videosurveillancesysteem, dat gekoppeld wordt aan gezichtsherkenningssoftware en een database met persoonlijke gegevens over alle 1,4 miljard Chinezen? Wat is uw mening over deze plannen?
Bent u op de hoogte van de berichtgeving van mensenrechtenorganisaties[2] die waarschuwen dat China surveillance-technologie inzet tegen iedereen die uit de pas loopt, zoals activisten, dissidenten en minderheden (één miljoen Oeigoeren)?[3]

Antwoord 4, 5
Berichten over dergelijke plannen zijn mij bekend. Zoals eerder aangegeven in antwoorden op vragen van het lid Ploumen (1 juli jl., kenmerk 2019Z12806) in het kader van Chinese plannen voor een nationaal sociaal kredietsysteem ziet het kabinet risico's voor de fundamentele vrijheden, privacy en mensenrechten van Chinese burgers en buitenlandse personen die zich in China bevinden. In Xinjiang is reeds sprake van diepgaande schendingen van privacy en andere mensenrechten door middel van geavanceerde surveillancetechnieken. Er zijn ook indicaties dat gezichtsherkenningssoftware buiten Xinjiang wordt ingezet om burgers te monitoren en categoriseren. Dit vormt een risico voor bepaalde etnische en/of religieuze groepen, mensenrechtenverdedigers en activisten van wie bekend is dat zij om hun (volgens internationale mensenrechtenverdragen legale) opvattingen, religie en/of gedragingen in China kunnen worden vervolgd of onderdrukt.

Vraag 6
Bent u het eens dat het onwenselijk is wanneer door Nederlandse bedrijven ontwikkelde en verkochte software wordt ingezet om bevolkingsgroepen te onderdrukken en mensenrechten te schenden?

Antwoord 6
Inzet van Nederlandse technologie voor het onderdrukken van bevolkingsgroepen of het schenden van mensenrechten acht het kabinet in alle gevallen onwenselijk. Nederlandse bedrijven die inspelen op de Chinese vraag naar geavanceerde technologie dienen zich te allen tijde rekenschap te geven van mogelijke ongewenste toepassingen van geleverde producten door Chinese afnemers. Bedrijven zijn zelf verantwoordelijk voor toepassen van *due diligence*. Zij dienen rekening te houden met de mogelijkheid dat Chinese partners een aandeel hebben in de totstandkoming van surveillancesystemen die beperking van fundamentele vrijheden van Chinese burgers tot gevolg hebben. In het geval van vergunningplichtige dual-usegoederen wijst de Nederlandse regering een vergunning af, indien er zorgen bestaan ten aanzien van het eindgebruik in relatie tot mensenrechtenschendingen.

---

[2] https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

[3] https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Vraag 7
Hebben Nederlandse technologiebedrijven een vergunningsplicht voor export van software die gebruikt kan worden voor gezichtsherkenning en emotieherkenning die ook ingezet kan worden voor predictive policing?

Antwoord 7
Nee.

Vraag 8
Op welke wijze voert Nederland op dit moment exportcontrole uit op cybersurveillance technologie? Wordt deze export aan een mensenrechtentoetsing onderworpen? Zo ja, op welke wijze? Voldoet deze controle naar uw oordeel om te voorkomen dat deze technologie ingezet kan worden om de mensenrechten te schenden?

Antwoord 8
Bepaalde cybersurveillancegoederen en -technologieën staan ingevolge het potentiële gebruik in civiele of militaire toepassingen onder exportcontrole. Dit geldt bijvoorbeeld voor de verkoop van technologie voor de ontwikkeling van *intrusion software*, software die gebruik maakt van kwetsbaarheden in systemen. Deze goederen zijn opgenomen in de controlelijst van de Europese dual-useverordening. Een bedrijf dat binnen de EU gevestigd is, is verplicht voor het exporteren van deze goederen en technologie buiten de EU een vergunning aan te vragen. Nederland keurt vergunningaanvragen af indien er zorgen bestaan ten aanzien van het eindgebruik in relatie tot mensenrechtenschendingen. Nederland spant zich internationaal in om aanvullend cybersurveillancegoederen in relatie tot mensenrechtenschendingen onder exportcontrole te brengen. Een voorbeeld hiervan zijn interceptie- en monitoringsystemen die veelal gebruikt worden door inlichtingendiensten. In het Wassenaar Arrangement vergt dit consensus van alle deelnemende landen.

Vraag 9, 10
Kunt u uiteenzetten wat de laatste stand van zaken is bij de herziening van de Europese dual-use verordening inzake de uitbreiding van exportcontrole op cybersurveillance goederen? Kunt u dit nader toelichten met uw appreciatie en de Nederlandse inzet?
Bent u het eens dat Nederlandse cybersurveillance technologie aan exportcontrole zou moeten worden onderworpen, en dat een mensenrechtentoets hier onderdeel van uit zou moeten maken? Bent u het eens dat dergelijke exportcontrole op Europees niveau zou moeten gelden?

Antwoord 9, 10
Nederland steunt de uitbreiding van exportcontrole op cybersurveillance goederen in relatie tot mensenrechtenschendingen in de herziening van de dual- useverordening. De in 2016 begonnen onderhandelingen in de Raad over de herziening van de dual-useverordening zijn moeizaam verlopen. Grootste discussiepunt in de onderhandelingen was voornoemde controle van cybersurveillancetechnologie. In december 2018 is gebleken dat geen gekwalificeerde meerderheid voor het onder controle brengen van cyber surveillance kon worden behaald om tot een Raadspositie te komen. Gelet op deze langdurige patstelling in de Raad en de gedeelde verantwoordelijkheid van de lidstaten om tot een eensgezind standpunt te komen, is de Raad in juni 2019 een mandaat overeengekomen tot onderhandeling met het Europese parlement. In dit mandaat is niet voorzien in aanvullende exportcontroleregelgeving op cybersurveillance technologie via de dual-useverordening.
Het is teleurstellend dat er geen overeenstemming in de Raad was om te komen tot een positie, waarbij de toevoeging van cybersurveillance technologie in relatie tot mensenrechtenschendingen is opgenomen. Nederland heeft zich hier zowel in de Raad als bilateraal actief voor ingezet en betreurt dat er op dit moment onvoldoende draagvlak voor is in de Raad. Nederland zal zich ervoor inzetten dat het onderwerp in de toekomst op de agenda blijft.
Het is onwenselijk nu vooruit te lopen op de nog onbekende uitkomst van het onderhandelingstraject tussen de Europese Raad, Europees parlement en de

Europese Commissie op het gebied van exportcontrole op bepaalde typen cybersurveillancegoederen.