Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Binnenhof 4
Den Haag

Rijnstraat 8
2515 XP Den Haag
Postbus 20061
Nederland
www.rijksoverheid.nl

Onze Referentie
BZDOC-1605772107-85
Uw Referentie
2019Z15231
Bijlage(n)

Datum 5 september 2019
Betreft Beantwoording vragen van de leden Van Ojik en Diks over de export van cybersurveillance technologie

Hierbij bied ik u, mede namens de minister van Buitenlandse Zaken, de antwoorden aan op de schriftelijke vragen gesteld door de leden Van Ojik en Diks (GroenLinks) over de export van cybersurveillance technologie. Deze vragen werden ingezonden op 18 juli 2019 met kenmerk 2019Z15231.

De Minister voor Buitenlandse Handel
en Ontwikkelingssamenwerking,

Sigrid A.M. Kaag

Antwoorden van de minister voor Buitenlandse Handel en Ontwikkelingssamenwerking, mede namens de minister van Buitenlandse Zaken, op vragen van de leden Van Ojik en Diks (GroenLinks) over de export van cybersurveillance technologie

Onze Referentie
BZDOC-1605772107-85

Vraag 1
Heeft u kennisgenomen van het bericht 'Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest'? 1)

Antwoord
Ja.

Vraag 2
Vindt u het wenselijk dat Nederlandse bedrijven dergelijke technologie leveren aan het Chinese ministerie van Openbare Veiligheid, wetende dat dit ministerie een belangrijke rol speelt bij het opzetten van de surveillancestaat in China en het onderdrukken van minderheden en tegenstanders van het regime?

Vraag 3
Vindt u het wenselijk dat Nederlandse bedrijven dergelijke technologie leveren aan Chinese bedrijven?

Antwoord vragen 2 en 3
Wat betreft toepassing van geavanceerde technologie voor cybersurveillance of gezichts- en emotieherkenning in China 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 vergaande schendingen van privacy en andere mensenrechten door middel van geavanceerde surveillancetechnieken.
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.

Vraag 4
Hoe beoordeelt u de reactie van de Chinese autoriteiten dat de technologie slechts wordt gebruikt voor trainingsdoeleinden? Vindt u dit geloofwaardig?

Antwoord
Het kabinet sluit niet uit dat de technologie ook voor andere dan trainingsdoeleinden wordt gebruikt.

Vraag 5
In hoeverre is de export van cybersurveillance technologie onderhevig aan een

vergunningplicht?

Antwoord
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 wijst 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 6
Wat is de huidige stand van zaken van de discussie in de Europese Raad over het voorstel van de Europese Commissie uit 2016 om de dual-useverordening te herzien?

Antwoord
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 blijven inzetten dat het onderwerp op de agenda blijft.

Vraag 7
In uw brief van 29 augustus 2018 schreef u dat het voorstel van de Europese Commissie nog vraagt om verdere uitwerking en een duidelijke afbakening van het begrip cybersurveillance technologie en dat Nederland zich inzet voor een controlelijst voor cybersurveillance technologie 2); vindt u dat gezichtsherkenningssoftware en emotieherkenningssoftware moeten worden opgenomen op de controlelijst?

Antwoord
Op EU niveau is besproken in hoeverre interceptie- en monitoringsystemen, zijnde cyber surveillance technologie, die veelal gebruikt worden door inlichtingendiensten gecontroleerd dienen te worden binnen de dual-useverordening.
Ten aanzien van andere opkomende technologieën die mogelijk ingezet kunnen worden voor surveillance doeleinden, zoals gezichtsherkenningssoftware en emotieherkenningssoftware, acht Nederland het onwenselijk dat schending van mensenrechten plaatsvindt met behulp van dergelijke technologieën. Voordat een nieuwe technologie onder exportcontroleregelgeving kan vallen, zal eerst vastgesteld moeten worden in hoeverre deze technologie zowel civiel als militair toepasbaar is. Dat gaat daarnaast om een goede afbakening van de technologie alsook de identificatie van potentiele risico's.

Vraag 8
Welke mogelijkheden ziet u om de Nederlandse export van cybersurveillance technologie aan landen waar zulke technologie mogelijk wordt ingezet bij mensenrechtenschendingen, aan banden te leggen, zolang consensus in de Europese Raad over herziening van de dual-useverordening uitblijft?

Vraag 9
Welke mogelijkheden ziet u op dit moment om een catch-all beschikking af te geven voor de export van cybersurveillance technologie en zo een ad-hoc vergunningplicht op te leggen?

Vraag 10
Welke mogelijkheden ziet u om, onder 5.4.4 in het hoofdstuk '30.06.00 Strategische goederen' uit het Handboek VGEM 3), bij ministeriële regeling een vergunningplicht in te stellen op de uitvoer van cybersurveillance technologie naar landen met autoritaire regimes waar de technologie mogelijk wordt gebruikt bij mensenrechtenschendingen?

Antwoord vragen 8, 9 en 10
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.

Een catch-all beschikking kan alleen worden afgegeven in een beperkt aantal gevallen. Dat geldt indien het risico aanwezig is dat de desbetreffende dual-usegoederen bestemd zijn voor inzet in massavernietigingswapens, of indien de eindbestemming van deze goederen een land betreft waarvoor een wapenembargo van toepassing is.

Op grond van de dual-useverordening (artikel 8) kan Nederland nationale wetgeving opstellen om een vergunningplicht in te stellen voor de uitvoer van dual-use items naar landen waar deze mogelijk worden ingezet bij mensenrechtenschendingen.

Ondanks het gegeven dat sommige (cyber)surveillance technologie niet onder de reikwijdte van de huidige verordening en het Nederlandse exportcontrolebeleid valt, is het kabinet van mening dat het bedrijfsleven een zelfstandige weloverwogen afweging dient te maken of de voorzetting van levering van de

goederen aan dergelijke eindgebruikers past binnen een adequaat compliance en MVO-beleid.