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-1449427758-58

Bijlage(n)

Datum 16 juli 2020
Betreft Antwoord op motie 35 207 nr. 27 van de leden van Ojik en Sjoerdsma over cybersurveillancetechnologie en exportcontrole

Geachte voorzitter,

Met deze brief ga ik graag nader in op de motie van de Leden van Ojik en Sjoerdsma (35 207, nr. 27, d.d. 8 oktober 2019), de brief aan uw Kamer (kamerstuk 32735, nr. 286, d.d. 4 februari 2020) en de recente toezegging van de minister van Buitenlandse Zaken in het notaoverleg mensenrechten (d.d. 22 juni 2020) om aan te geven of surveillance-apparatuur dual-use is.

Net als uw Kamer wil het kabinet betrokkenheid van (Nederlandse) bedrijven bij de inzet van cybersurveillancegoederen en -technologie bij de schending van mensenrechten voorkomen. Daartoe zet het kabinet zich in om dit type goederen onder exportcontrole te brengen, wanneer dit nog niet het geval is. Hierin trekt Nederland samen op met andere landen in Europees en breder internationaal verband. Exportcontrolemaatregelen zijn immers pas effectief wanneer meerdere landen zich committeren om de export van bepaalde goederen te controleren en zo de vrije beschikbaarheid op de markt te beperken in geval er sprake is van ongewenst eindgebruik. Ook houdt het kabinet op deze manier oog voor een gelijk speelveld in Europa en daarbuiten.

In het Wassenaar Arrangement (WA), het exportcontroleregime voor dit type goederen, werd eind 2019 een belangrijke stap gezet. In aanvulling op reeds gecontroleerde cybersurveillancegoederen is door de 42 aangesloten landen besloten om ook programmatuur voor cybersurveillance onder exportcontrole te brengen. Het gaat daarbij om de toevoeging van onder andere monitoringcentra die communicatie van computer- en telecomnetwerken kunnen monitoren en analyseren, gericht op het volgen van personen en groepen. Deze wijzigingen worden dit jaar overgenomen in de EU dual-useverordening bij de jaarlijkse actualisering van de controlelijsten. Hiermee geeft het kabinet opvolging aan de motie van de Leden van Ojik en Sjoerdsma om cybersurveillancetechnologie in Europees verband verder onder exportcontrole te brengen.

Voorts lopen in Brussel nog de onderhandelingen over de herziening van de EU dual-useverordening tussen de Raad, de Commissie en het Europees Parlement. Zoals eerder aan uw Kamer vermeld (Kamerstuk 3894, 10 september 2019) zijn de in 2016 begonnen onderhandelingen in de Raad over de herziening van de EU

dual-useverordening moeizaam verlopen. Grootste discussiepunt in deze onderhandelingen was voornoemde controle van cybersurveillancetechnologie. Het bleek niet mogelijk om in de Raad op dit punt overeenstemming te bereiken. Gelet op de langdurige patstelling in de Raad en de gedeelde verantwoordelijkheid van de lidstaten om tot een eensgezind standpunt te komen, kwam de Raad in juni 2019 een mandaat overeen tot onderhandeling met het Europees Parlement. In dit mandaat is, ondanks Nederlandse inzet, helaas niet voorzien in aanvullende exportcontroleregelgeving op cybersurveillancetechnologie via de dual-useverordening. Uit de voortgaande onderhandelingen blijkt dat het Europees Parlement vast blijft houden aan de wens om cybersurveillancetechnologie expliciet in de dual-useverordening op te nemen. Ook in de Raad is dit een terugkerend thema van gesprek. Nederland blijft zich inzetten voor het opnemen van cybersurveillancetechnologie in relatie tot mensenrechtenschendingen in de dual-useverordening.

Om helderheid te scheppen over de exacte reikwijdte van de EU dual-useverordening op het gebied van exportcontrole van cybersurveillancetechnologie geeft het kabinet in deze brief – aan de hand van twee groepen – een nadere toelichting op welke technologie na de actualisatie van de EU controlelijst later dit jaar onder exportcontrole valt en welke niet.

Technologie gecontroleerd onder de EU dual-useverordening
De eerste groep betreft items die reeds gecontroleerd worden onder de dual-useverordening of op korte termijn gecontroleerd gaan worden. Dit betreft cybersurveillancegoederen die worden ingezet voor het onderscheppen (interceptie) of verstoren van communicatienetwerken (telecom en computer). Dit kan zowel via apparatuur als inbraakprogrammatuur (*intrusion software*).
Zoals hiervoor genoemd, zal deze groep van items dit jaar uitgebreid worden met aanvullende programmatuur voor het onderscheppen en analyseren van communicatie van computer- en telecomnetwerken gericht op het volgen en monitoren van personen. Bovengenoemde cybersurveillancetechnologieën kennen geen andere toepassingen en worden gebruikt door inlichtingen- en politiediensten. Naast een legitiem, rechtmatig en democratisch gecontroleerd gebruik, bestaat er ook een risico dat deze goederen op ongewenste wijze ingezet worden met als gevolg mensenrechtenschendingen. Daarnaast bestaat een grote categorie gecontroleerde goederen gericht op informatiebeveiliging. Deze apparatuur is primair bedoeld voor het beveiligen van informatie via netwerken door middel van encryptie. Hoewel deze goederen niet direct zijn ontworpen voor cybersurveillancedoeleinden, is niet bij voorbaat uit te sluiten dat zij in een toepassing wel voor deze doeleinden ingezet worden, zoals bijvoorbeeld het gebruik van *Deep Packet Inspection*.

Niet-gecontroleerde technologie
Snelle technologische ontwikkelingen leiden ertoe dat er op het gebied van cybersurveillancetechnologie nieuwe toepassingen ontwikkeld zijn, die (nog) niet onder exportcontrole vallen. Dat gaat veelal om technologieën die niet primair worden ontwikkeld ten behoeve van surveillance, maar een veel bredere toepassing kennen. Zo kunnen ontwikkelingen op het gebied van kunstmatige intelligentie en gezichtsherkenningssoftware onder deze tweede groep geschaard worden. Naast vele legitieme toepassingen, roepen deze nieuwe technologieën ook vragen op ten aanzien van onrechtmatig gebruik en mogelijke inzet bij mensenrechtenschendingen.

Nederlandse inzet
Bij vergunningaanvragen voor export van de eerste groep gecontroleerde goederen, programmatuur en technologie toetst het kabinet expliciet het risico op mensenrechtenschendingen. Indien zorgen bestaan ten aanzien van het eindgebruik of de eindgebruiker in relatie tot mensenrechtenschendingen, wordt een vergunningaanvraag afgewezen. Ook eist het kabinet van bedrijven een *internal compliance program* voor bepaalde vergunningen. Hierin moet expliciet beschreven staan welke inspanningen een bedrijf onderneemt om risico's op mensenrechtenschendingen te minimaliseren.

De regering voert ook gesprekken met bedrijven waarvan bekend is dat zij in deze sector actief zijn, in het bijzonder wanneer de hierboven geïdentificeerde goederen en technologie niet onder een vergunningplicht vallen. Bedrijven worden nadrukkelijk gewezen op de risico's die met hun bedrijfsactiviteiten gepaard gaan. Het kabinet verwacht van deze bedrijven dat zij een weloverwogen afweging maken of (de voorzetting van) levering van de goederen aan bepaalde eindgebruikers past binnen een adequaat compliance- en IMVO-beleid, in lijn met de OESO-richtlijnen voor multinationale ondernemingen en de *UN Guiding Principles on Business and Human Rights*.

Nederland zal zich in de Europese Unie blijven inzetten voor het opnemen van EU exportcontroleregelgeving ten aanzien van cybersurveillancetechnologie in relatie tot mensenrechtenschendingen. Ten aanzien van nieuwe ontwikkelingen op het gebied van cybersurveillance (zoals gezichtsherkenningssoftware) is het kabinet voornemens om nader onderzoek in te stellen naar de aard en de toepassingen van dit soort technologieën, naar het risico op hun bijdrage aan mensenrechtenschendingen en gericht op de mogelijkheden om dit type technologie via vastgestelde parameters onder exportcontrole te brengen. Dat vergt onder andere advies van gespecialiseerde externe partijen en van het bedrijfsleven zelf. Met het oog op een level-playing-field en een effectief exportcontrolebeleid, zal Nederland daar ook in Europees en internationaal verband consultaties over voeren en hier samen met andere landen in optrekken. Tevens zal in Europees verband verkend worden of en in hoeverre het mogelijk is om samen met andere Europese lidstaten de export van (cyber)surveillance-technologie in kaart te brengen. Daarbij blijven dezelfde overwegingen meespelen die ik eerder aan uw Kamer reeds genoemd heb (kamerstuk 32735, nr. 286, d.d.), waaronder de bedrijfsvertrouwelijke en concurrentiegevoelige aard van dit soort informatie.

Zoals hierboven gesteld, kan ik u verzekeren dat ten aanzien van de door de dual-useverordening gecontroleerde cybersurveillancegoederen en –technologieën, het kabinet te allen tijde een gedegen mensenrechtentoets uitvoert op vergunningaanvragen en dat bedrijven en organisaties worden aangesproken op hun IMVO-beleid.

Onze Referentie
BZDOC-1449427758-58

De Minister voor Buitenlandse Handel
en Ontwikkelingssamenwerking,

Sigrid A.M. Kaag