

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

### 476

Vragen de leden **Rajkowski** en **Minhas** (beiden VVD) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Infrastructuur en Waterstaat over *het bericht «ProRail dumpst Chinese bewakingscamera's, de NS laat ze hangen»* (ingezonden 12 september 2022).

Antwoord van Staatssecretaris **Heijnen** (Infrastructuur en Waterstaat) en van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 24 oktober 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 202.

#### Vraag 1

Bent u bekend met het bericht «ProRail dumpst Chinese bewakingscamera's, de NS laat ze hangen»?<sup>1</sup>

#### Antwoord 1

Ja, wij zijn bekend met het bericht.

#### Vraag 2

Klopt het bericht dat de NS duizenden nieuwe Chinese camera's heeft besteld? Zo ja, hoe beoordeelt u dit?

#### Antwoord 2

De camera's vormen onderdeel van een Europese aanbesteding voor de modernisering van de materieelserie VIRM2/3 en een Europese aanbesteding van de nieuwbouw van de materieelserie ICNG. Deze aanbestedingen zijn gegund aan Europese treinfabrikanten, die op hun beurt voor een deel van deze levering gebruik maken van Chinese onderleveranciers.

NS heeft bij de Staatssecretaris van IenW aangegeven dat zij diverse maatregelen heeft getroffen zodat (statelijke) actoren niet van buitenaf bij de inhoud of de besturing van de camera's kunnen komen. Eén van de maatregelen is dat deze camera's zich bevinden in een afgesloten en beveiligd (intern) netwerk dat niet is gekoppeld aan het internet. Dit betekent volgens NS dat niemand van buitenaf bij de inhoud of besturing van de camera's kan komen. Daarnaast heeft NS bij de Staatssecretaris aangegeven gebruik te maken van de adviezen van de rijksoverheid, zie ook het antwoord op vraag 7.

<sup>1</sup> Follow the Money, 6 september 2022, «ProRail dumpst Chinese bewakingscamera's, de NS laat ze hangen», <https://www.ftm.nl/artikelen/ns-prorail-en-chinese-cameras>.

### Vraag 3

Op welke plekken heeft de NS momenteel Chinese camera's hangen en op welke plekken komen de Chinese camera's nog te hangen? Hoeveel Chinese camera's hangen er op dit moment binnen treinen en op en rondom stations?

### Antwoord 3

NS heeft geen camera's van Chinese makelij op stations. Momenteel gebruikt NS camera's van Chinese makelij alleen in een aantal type treinen. Na modernisering bevat de materieelserie VIRM 2/3 camera's van Chinese makelij evenals de (nieuwe) materieelserie ICNG.

### Vraag 4

Welke eisen gaat u opnemen in de nieuwe Hoofdrailnetconcessie ten aanzien van het gebruik van Chinese camera's op stations en in treinen?

### Antwoord 4

In het Programma van Eisen vraagt de Staatssecretaris van IenW de beoogd concessiehouder, een rol te spelen op het gebied van terrorismebestrijding, o.a. door het beschikbaar hebben van cameratoezicht in de trein. De Staatssecretaris van IenW vindt het belangrijk om de beoogd concessiehouder vrij te laten in de bedrijfsvoering, opdat zij haar kennis en expertise optimaal kan benutten. Er is daarom gekozen voor outputsturing waar het kan en inputsturing waar ik dat nodig acht met het oog op de maatschappelijke meerwaarde. Het meegeven van specificaties voor het type te gebruiken camera's past daar niet in. Ook hanteert NS nu ook al de adviezen van de rijksoverheid, zie ook het antwoord op vraag 7.

### Vraag 5

Bent u ervan op de hoogte dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vervoer van personen en goederen over (hoofd-)spoorweginfrastructuur aanmerkt als vitale infrastructuur? Zo ja, hoe weegt u de aanschaf van producten en diensten van landen met een offensieve cyberstrategie gericht tegen Nederland in de vitale infrastructuur?

### Antwoord 5

Ja. Voor het identificeren van vitale processen zijn de betrokken Ministers van vakdepartementen verantwoordelijk. Het proces vervoer van personen en goederen over de (hoofd)spoorweginfrastructuur is door de Minister van Infrastructuur en Waterstaat aangemerkt als een vitaal proces<sup>2</sup>. Dit betekent dat aanbieders van een dienst binnen dit proces kunnen worden aangemerkt als vitale aanbieder en aanbieder van een essentiële dienst (AED), waarmee ze onder het regime van de Wet bescherming netwerk- en informatiesystemen (Wbni) vallen. Zie ook het antwoord op vraag 7.

### Vraag 6

Deelt u de mening dat het zeer onwenselijk is dat de NS camera's inzet en aankoopt die worden gemaakt door Chinese techbedrijven die deels in handen zijn van de Chinese staat? Zo ja, in hoeverre zit het kabinet strak op de aanbestedingen uit landen met een offensief cyberprogramma (onder andere China) bij organisaties waar de overheid aandelen in heeft? Zo nee, waarom niet?

### Antwoord 6

Ten aanzien van de inkoop van producten en diensten is het overheidsbeleid dat nationale veiligheidsoverwegingen worden meegewogen. Ter ondersteuning van dit beleid zijn er instrumenten voor de rijksoverheid, medeoverheden en vitale aanbieders ontwikkeld die organisaties handvatten bieden bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's, waarbij het Rijk gevraagd en ongevraagd advies en ondersteuning kan bieden.

<sup>2</sup> Zie Kamerstuk 29 826, nr. 108.

Zo wordt bij de aanschaf en implementatie van gevoelige apparatuur rekening gehouden met eventuele risico's in relatie tot de leverancier (zoals een offensief cyberprogramma gericht tegen Nederland), en met risico's die zich kunnen voordoen het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Daarbij kunnen als mitigerende maatregelen bijvoorbeeld strenge eisen worden gesteld door de opdrachtgever aan de (informatie)beveiliging van producten en diensten. Zie ook het antwoord op vraag 7.

#### Vraag 7

Geeft de rijksoverheid adviezen aan derde belanghebbenden die deel uitmaken van de door de NCTV gekwalificeerde vitale infrastructuur over de aanschaf van camera's? Zo ja, hoe zou de aanschaf van de Chinese camera's door de NS passen in het advies van de rijksoverheid? Zo nee, waarom niet?

#### Antwoord 7

Vitale aanbieders zijn onder meer op basis van wetgeving, waaronder de Wbni, verplicht tot het treffen van passende maatregelen ter beveiliging van hun netwerk- en informatiesystemen (zorgplicht). Ook dienen zij inzicht te hebben in de risico's die hun dienstverlening ten aanzien van het vitale proces kunnen raken.

Vitale aanbieders zijn daarbij zelf verantwoordelijk voor het treffen van de juiste maatregelen. Sectorale toezichthouders houden toezicht op de wijze waarop vitale aanbieders invulling geven aan deze zorgplicht.

Ten aanzien van de inkoop van producten en diensten is het overheidsbeleid dat nationale veiligheidsoverwegingen worden meegewogen. Ter ondersteuning van dit beleid zijn er instrumenten voor de rijksoverheid, medeoverheden en vitale aanbieders ontwikkeld die organisaties handvatten bieden bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's, waarbij het Rijk gevraagd en ongevraagd advies en ondersteuning kan bieden.

Zo wordt bij de aanschaf en implementatie van gevoelige apparatuur rekening gehouden met eventuele risico's in relatie tot de leverancier (zoals een offensief cyberprogramma gericht tegen Nederland), en met risico's die zich kunnen voordoen in het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Daarbij kunnen als mitigerende maatregelen bijvoorbeeld strenge eisen worden gesteld door de opdrachtgever aan de (informatie)beveiliging van producten en diensten. NS heeft bij de verwerving van de camera's, in lijn met dit beleid, nationale veiligheidsrisico's meegewogen aan de hand van het genoemde instrumentarium en hiertoe nadere maatregelen getroffen zoals toegelicht in het antwoord op vraag 2.

#### Vraag 8

Klopt het bericht dat het Nationaal Cyber Security Centrum (NCSC) nog geen negatief advies heeft gegeven over de merken Dahua en Hikvision? Zo ja, waarom is er tot op heden nog geen negatief advies gegeven? Zo nee, wat is hiervoor nodig?

#### Antwoord 8

Het NCSC geeft geen advies over individuele producten of diensten. Het NCSC raadt organisaties aan om risicomanagement te implementeren in hun organisatie en dit ook toe te passen bij het aanschaffen van producten en diensten. De risico's die verbonden zijn aan bepaalde producten of diensten zijn erg afhankelijk van hoe een product of dienst wordt ingezet bij een individuele organisatie. Om daar duidelijkheid over te krijgen adviseert het NCSC om een specifieke risicoanalyse uit te voeren. Hiermee kan op basis van dreigingen, de te beschermen belangen, nationale veiligheidsoverwegingen en mogelijke maatregelen een risicoafweging worden gemaakt. Daardoor kan een passend pakket aan weerbaarheidsmaatregelen geïmplementeerd worden. Vitale aanbieders zijn hier zelf verantwoordelijk voor.

#### Vraag 9

Bent u het ermee eens dat het onacceptabel is dat miljoenen Nederlanders worden gefilmd door omstreden Chinese camera's waarvan niet duidelijk is wat er met deze beelden wordt gedaan? Zo ja, welke stappen bent u bereid te zetten om ervoor te zorgen dat deze Chinese camera's er niet komen?

#### Antwoord 9

De toepassing van camera's in de openbare ruimte en op stations hebben een rol in het borgen van veiligheid voor het publiek dat daar aanwezig is. Zoals ook aangegeven in het antwoord op vraag 2 heeft NS diverse maatregelen getroffen zodat statelijke actoren niet van buitenaf bij de inhoud of de besturing van de camera's kunnen komen.

Nederland en de EU spreken in verschillende verbanden, waaronder binnen de VN, met China over dataveiligheid. Centraal hierbij staat de bescherming van privacy, zoals de naleving van de Algemene verordening gegevensbescherming (AVG), bescherming van mensenrechten en het tegengaan van ongepaste toegang van overheden tot datagegevens. Zoals aangegeven in de Notitie<sup>3</sup> «Nederland-China: Een nieuwe balans» 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.

Op grond van de Algemene Verordening Gegevensbescherming (AVG) gelden er regels voor de verwerking van persoonsgegevens, zo ook wanneer de verwerking plaatsvindt door middel van camerabeelden. Het is aan de verwerkingsverantwoordelijke om deze wettelijk verplichte regels in acht te nemen. Daartoe behoort dat de verwerking van persoonsgegevens goed is beveiligd. Ook staat de AVG de doorgifte van persoonsgegevens aan derde landen niet dan onder strikte voorwaarden toe. Doorgifte is namelijk slechts toegestaan op grond van een van de wettelijke bepalingen uit hoofdstuk V van de AVG. Aangezien voor China geen door de Europese Commissie genomen adequaatheidsbesluit bestaat, waarin wordt besloten dat dit land een passend beschermingsniveau waarborgt, kan structurele doorgifte van persoonsgegevens alleen plaatsvinden voor zover er door de verwerkingsverantwoordelijke «passende waarborgen» worden geboden. Het is aan de Autoriteit Persoonsgegevens (AP), de toezichthouder op de AVG, om erop toe te zien dat er passende waarborgen zijn getroffen. Als dit niet het geval is heeft de AP onder meer de bevoegdheid om boetes op te leggen, maar ook om de verwerking te verbieden.

#### Vraag 10

Wanneer kan de Kamer de uitvoering van de aangenomen motie Rajkowski en Van Weerdenburg (Kamerstuk 26 643, nr. 830) en de uitvoering van de overgenomen motie Rajkowski c.s. (Kamerstuk 26 643, nr. 874) verwachten?

#### Antwoord 10

Zoals verzocht in de overgenomen motie<sup>4</sup> Rajkowski c.s. zal de Kamer nog voor het kerstceces geïnformeerd worden over de verzochte richtlijn voor de rijksoverheid en haar leveranciers, om producten of diensten van organisaties en bedrijven uit landen met een offensieve cyberagenda gericht tegen Nederland uit bepaalde aanbestedingen te kunnen weren. Hierin wordt ook meegenomen de toezegging aan de Kamerlid Rajkowski voor een onderzoek over hoe dit zou kunnen, zoals gedaan in het debat met de Commissie Digitale Zaken over de digitale overheid, datagebruik en algoritmen, digitale identiteit van 22 maart 2022. Op 5 april 2022 is de motie<sup>5</sup> van de leden Rajkowski en Van Weerdenburg aangenomen die het kabinet verzoekt een scan uit te voeren op de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in de vitale infrastructuur. Op dit moment wordt door het Ministerie van Justitie en Veiligheid, in samenwerking met de betrokken

<sup>3</sup> Zie Kamerstuk 35 207, nr. 1.

<sup>4</sup> Zie Kamerstuk 26 643, nr. 874.

<sup>5</sup> Zie Kamerstuk 26 643, nr. 830.

departementen, verkend op welke manier opvolging kan worden gegeven aan de deze motie.