

SCHRIFTELIJKE VRAAG

nr. 264

van **FILIP BRUSSELMANS**

datum: 17 maart 2022

aan **JAN JAMBON**

MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BUITENLANDSE ZAKEN, CULTUUR, DIGITALISERING EN FACILITAIR MANAGEMENT

Cyberveiligheid - Camera's in Vlaamse overheidsgebouwen

De Nederlandse televisiezender NOS meldt na eigen onderzoek dat Nederland vol hangt met camera's van omstreden Chinese fabrikanten Hikvision en Duhua, onder meer bij hun ministerie van Buitenlandse Zaken.

De fabrikanten worden verdacht van spionage en mensenrechtenschendingen. Via een zogenoemd ingebouwd 'achterdeurtje' kunnen kwaadwilligen meekijken met de camera's, bijvoorbeeld bij een ministerie waar dagelijks diplomaten en politici binnengaan. In China is het immers verplicht gegevens te delen met de overheid indien zij erom verzoeken.

1. Is de minister bekend met de problematiek van camera's en andere apparatuur van Chinese bedrijven, zoals Hikvision of Dahua?
2. Worden deze camera's ook gebruikt in Vlaamse overheidsgebouwen? Zo ja, om hoeveel camera's gaat het? Waar staan die camera's?
3. Aan welke eisen, die betrekking hebben op cyberspionage, wordt getoetst bij de aanschaf van camera's bij overheidsgebouwen? Voldoen de camera's van Hikvision en Dahua aan deze eisen?
4. Is het technisch mogelijk voor China om mee te kijken, live of achteraf? Zo ja, hoe dan? Zo niet, is die mogelijkheid er helemaal niet of is ze softwarematig dichtgezet?
5. Hoe groot acht de minister de kans dat China meekijkt of mee heeft gekeken via deze camera's als ze aanwezig zouden zijn? Op basis waarvan maakt de minister deze inschatting?
6. In de Verenigde Staten is de inzet van Hikvision- en Dahua-camera's bij overheidsgebouwen verboden. Daarnaast heeft het Europees Parlement eerder besloten om camera's van Hikvision niet meer te gebruiken.

Is dit in Vlaanderen ook het geval?

7. Deelt de minister de mening dat bedrijven uit staten die een offensief cyberprogramma tegen Vlaanderen uitvoeren, niet geschikt zijn om camera's te leveren die zijn opgesteld bij organisaties die een aantrekkelijk doelwit vormen voor een dergelijk offensief programma?
8. Zijn er Europese alternatieven in de markt? Zo, ja is de minister het eens met het standpunt dat het verstandig kan zijn om die in te zetten? Zo niet, is hij het ermee eens dat het wenselijk is dat er Europese alternatieven zijn, ook op het gebied van technologie?

9. Is de minister het ermee eens dat we de cyberdreiging vanuit China ernstig moeten nemen en daarom kritisch moeten kijken naar de aanschaf en inzet van niet-Europese hardware en software voor gevoelige zaken zoals het filmen van overheidsgebouwen? Zo ja, welke stappen gaat de minister ondernemen? Zo niet, waarom niet?
10. Is de minister van plan met China in gesprek te treden over het belang van privacy- en veiligheidsstandaarden in technologie en dat toegang van de Chinese staat tot gevoelige data niet acceptabel is?

JAN JAMBON

MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BUITENLANDSE ZAKEN,
CULTUUR, DIGITALISERING EN FACILITAIR MANAGEMENT

ANTWOORD

op vraag nr. 264 van 17 maart 2022

van **FILIP BRUSSELMANS**

1. Ik ben mij inderdaad bewust van deze problematiek omtrent elektronische apparatuur, maar deze problematiek is niet beperkt tot camera's of enkel Chinese bedrijven. Ik streef daarom naar het systematisch verhogen van het bewustzijn van cyberrisico's bij de Vlaamse overheid.
2. Ja, deze camera's worden ook gebruikt bij Vlaamse overheidsgebouwen. Als aanbestedende overheid moeten we immers de regelgeving overheidsopdrachten, en de erin vastgelegde principes van gelijke behandeling en non-discriminatie, respecteren zoals u verder ook kan lezen in het antwoord op vragen 6 t.e.m. 9. Uit veiligheidsoverwegingen kan ik u geen lijst bezorgen, maar ik kan u wel zeggen dat Het Facilitair Bedrijf weet heeft van 493 camera's van Dahua en Hikvision, verspreid over 29 gebouwen/sites in beheer.
3. Voor de aankoop camerabewakingssystemen en camera's worden er een heel aantal technische vereisten en technische functionaliteiten (waaronder bv. vereiste tot authenticatie met een VO eigen authenticatieserver (802.1x protocol)) opgenomen in de aanbestedingsdossiers. Zowel Hikvision als Dahua voldoen aan deze eisen. Controle op mogelijke cyberspionage van alle en/of geselecteerde cameramerken is echter zeer specifiek en er zal hiervan in de technische specificaties van de toestellen nergens een spoor terug te vinden zijn.

De overheidsopdrachtenwetgeving bepaalt bovendien dat de principes van gelijke behandeling en non-discriminatie moeten gerespecteerd worden. Voorafgaand toetsen van "enkel" Hikvision en Dahua is niet toegestaan.

Uiteraard werden wel een aantal technische maatregelen in het veelgebruikte raamcontract "bekabeling en elektrotechnische installatiewerken" opgenomen, zoals:

- "De beeldtransmissie is beveiligd";
- "De beheerssoftware kan enkel geconsulteerd worden via authenticatie. Er zijn meerdere niveaus van consultatie mogelijk, met eigen authenticatie."

Voor deze opdrachten van Het Facilitair Bedrijf zijn ook telkens de informatieclassificatievereisten van de Vlaamse overheid rond de inrichting van netwerken, het opslaan, verzenden en raadplegen van data(beelden) van toepassing.

Bovendien valt ook op te merken dat het niet zozeer het toestel zelf is, maar de mogelijkheid om deze toestellen te bereiken via een netwerkaansluiting vanaf het internet die het zwakke punt vormt. Ook hieraan wordt tegemoet gekomen door middel van de nodige technische maatregelen, die u kan terugvinden bij het antwoord op vragen 4 en 5.

- 4-5. De camerabewaking besteld door Het Facilitair Bedrijf wordt volgens volgende principes ingericht:
 - Deze toestellen worden steeds aangesloten op een specifiek daartoe ingericht (fysiek of virtueel) netwerk;

- Dit netwerk vereist een expliciete identificatie van de gekoppelde camera's. Het is dus niet mogelijk om een onbekend toestel te koppelen met hetzelfde netwerk dan deze camera's;
- Dit netwerk is gescheiden per gebouw;
- Dit netwerk is gescheiden van alle ander netwerkgebruik;
- Dit netwerk is niet gekoppeld aan het internet.

Bovenstaande principes reduceren maximaal de risico's op misbruik van deze toestellen.

Gezien deze beveiliging en het feit dat mijn administratie geen enkele indicatie van hacking heeft, acht ik de kans dat China meekijkt of mee heeft gekeken dan ook bijzonder klein, zelfs onwaarschijnlijk.

6-9. Het gebruik van camera's van Hikvision en Dahua is momenteel niet verboden, Vlaanderen is immers geen voorstander van het gebruik van zwarte lijsten. De aankoop van werken, goederen en diensten gebeurt namelijk binnen het kader van de regelgeving overheidsopdrachten.

Hierbij moeten onder meer de beginselen van non-discriminatie en gelijke behandeling worden gerespecteerd. Dit betekent dat de participatie van ondernemingen uit andere EU-lidstaten niet mag worden verhinderd of bemoeilijkt. Voor ondernemingen uit derde landen (niet-EU-lidstaten) is de toegang tot de Europese aanbestedingsmarkt afhankelijk van internationale overeenkomsten, maar de vaststelling is dat deze bedrijven veelal aan overheidsopdrachten deelnemen door middel van hun in Europa gevestigde rechtspersonen of als toeleverancier van een in Europa gevestigde inschrijver.

Het opstellen van een 'zwarte lijst' met buitenlandse bedrijven en technologie zou dan ook op gespannen voet staan met deze beginselen inzake non-discriminatie en gelijke behandeling. Dit neemt niet weg dat bij bepaalde overheidsopdrachten moet worden nagegaan of er een nationale veiligheidsdimensie is. Dit zal sterk afhankelijk zijn van de sector en het type product of dienst dat geleverd moet worden.

Nationale veiligheidsrisico's kunnen onder meer aan de orde zijn indien een overheidsopdracht impact heeft op vitale infrastructuur, de strategische onafhankelijkheid of het doorgeven van vertrouwelijke informatie. In dergelijke gevallen moet een risicoanalyse worden uitgevoerd die ervoor zorgt dat de nodige maatregelen worden getroffen om deze risico's af te dekken.

Voor bedrijven die betrokken zijn bij een overheidsopdracht, dient geval per geval te worden nagegaan wat de antecedenten zijn van dat bedrijf, en wat de relatie is tussen de aard van die producten, het beoogde eindgebruik en de mogelijke veiligheidsrisico's.

Zo verplicht de regelgeving overheidsopdrachten om in de selectiefase de betrouwbaarheid en de geschiktheid van ondernemingen na te gaan.

In de technische bepalingen en uitvoeringsvoorwaarden van de overheidsopdracht kunnen allerlei maatregelen en garanties worden opgenomen om deze veiligheidsrisico's uit te sluiten (zie ook het antwoord op vragen 3 en 4-5).

Bovenstaande toont dus aan dat de regelgeving overheidsopdrachten de nodige ruimte biedt om beheersingsmaatregelen te nemen bij opdrachten met bepaalde veiligheidsrisico's.

Dit veronderstelt evenwel dat voorafgaand aan de opdracht een degelijke risicoanalyse is uitgevoerd.

Ik ben mij er uiteraard van bewust dat andere landen spionageactiviteiten ontwikkelen, op heel wat domeinen. Daar moeten we heel aandachtig en beducht voor zijn. Vlaanderen onderhoudt dan ook goede relaties met de federale

veiligheidsdiensten, onder meer omdat we het belangrijk vinden om dergelijke mogelijke spionagerisico's in te dijken.

Daarnaast streeft Vlaanderen zelf ook naar een efficiënte veiligheidscultuur waarbij we waken over onze strategische veiligheidsbelangen.

10. In Vlaanderen is de toegang tot gevoelige data door niet-gemachtigden onaanvaardbaar. Dat geldt voor, of potentieel in opdracht van, de Chinese staat, maar evenzeer voor andere actoren of entiteiten. Op dit ogenblik heb ik daartoe nog geen gesprek gepland.