

SCHRIFTELIJKE VRAAG

nr. 382

van **SABINE DE BETHUNE**

datum: 5 april 2018

aan **LIESBETH HOMANS**

VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BINNENLANDS BESTUUR, INBURGERING, WONEN, GELIJKE KANSEN EN ARMOEDEBESTRIJDING

Vlaamse overheid - Bescherming data tegen cyberdreigingen

Op 6 maart 2018 heb ik aan minister-president Bourgeois een vraag om uitleg (nr. 1320) gesteld over de digitale machtsgreep van China en de gevolgen ervan voor het Vlaamse beleid inzake cyberveiligheid. Hij gaf mij een beperkt antwoord en verwees mij door naar de minister van Binnenlands Bestuur om een ruimer antwoord te krijgen over de interne Vlaamse maatregelen.

In De Standaard van 26 februari wordt gemeld dat China een sterke invloed heeft op het Belgische telecomnetwerk: zo draaien alle Belgische telecomnetwerken (Orange, Proximus en Base) op Chinese hardware. Volgens kenners zijn wij het enige land in West-Europa waar dat het geval is.

Volgens de experts zou China via deze weg toegang willen krijgen tot zo veel mogelijk data. Want data zullen vandaag, maar ook in de toekomst, één van de meest gewilde handelswaren zijn. Zo waarschuwden de FBI en de CIA deze maand al voor het gevaar van het gebruik van Chinese smartphones.

Om dit mogelijk te maken, zet het land sterk in op het verwerven van een machtspositie in de telecomsector via Chinese bedrijven, zoals Huawei, die volop bezig zijn met de ontwikkeling van het 5G-netwerk waardoor bedrijven in de toekomst hun producten met het internet kunnen verbinden. Op deze wijze zullen deze Chinese bedrijven ook toegang krijgen tot de data van bijvoorbeeld zelfrijdende auto's of onderdelen van nutsvoorzieningen.

De VS en onze omringende landen onderzoeken momenteel hoe de buitenlandse toegang tot essentiële infrastructuur kan worden tegengehouden. In de Verenigde Staten is het na alarmerende rapporten van de Amerikaanse veiligheidsdiensten al sinds 2012 de facto verboden om samen te werken met Huawei en ZTE. In Frankrijk is de wet die de operatoren van vitaal belang onder streng toezicht van het leger plaatst, verstrengd. Ook Groot-Brittannië, Duitsland en Nederland zoeken naar middelen om eigen data beter te beschermen.

1. Welke maatregelen werden tot op heden genomen in de bescherming van data van de Vlaamse overheidsdepartementen?
2. In welke mate werden Vlaamse overheidsnetwerken en essentiële infrastructuur reeds het slachtoffer van cyberaanvallen? In het bijzonder vanuit China?

3. In welke mate is er enig overleg met de federale minister van Telecom en Digitale Agenda, de federale minister van Binnenlandse Zaken en met de bevoegde ministers van de andere deelstaten? Indien niet, acht de minister het opportuun om dergelijk overleg op te starten? Zal zij ter zake zo nodig zelf het initiatief nemen?
4. Zal de Vlaamse Regering een rapport publiceren over ICT-infrastructuur en cyberdreigingen in Vlaanderen?

LIESBETH HOMANS

VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BINNENLANDS BESTUUR, INBURGERING, WONEN, GELIJKE KANSEN EN ARMOEDEBESTRIJDING

ANTWOORD

op vraag nr. 382 van 5 april 2018

van **SABINE DE BETHUNE**

1. Cybercriminaliteit, de veiligheid en de regulering van de Telecomsector is federale materie en de veiligheid van telecomnetwerken is natuurlijk in de eerste plaats de verantwoordelijkheid van de telecombedrijven zelf.

Voor wat betreft mijn bevoegdheden, namelijk de gemeenschappelijke ICT-infrastructuur en telecomdiensten van de Vlaamse overheid, verwijs ik naar mijn antwoorden op eerdere schriftelijke vragen (SV), namelijk SV nr. 427 (9 maart 2016) van de heer Marnic De Meulemeester en SV nr. 437 (11 maart 2016) van de heer Chris Janssens. Ik verwijs ook naar de bespreking van mijn beleidsbrief 2016-2017.

(zie p. 62: <http://docs.vlaamsparlement.be/pfile?id=1225578>)

Verder spreekt het voor zich dat we bij de aanbesteding van telefonie- en ICT-diensten maatregelen vragen aan onze dienstverleners op het vlak van de beveiliging, om te voorkomen dat derden ongeoorloofd toegang krijgen tot het netwerk en onze data.

2. Zie het antwoord op de SV nr. 437 (11 maart 2016) van de heer Chris Janssens. De cijfers in dit antwoord en de bijhorende duiding zijn nog actueel.

'Attributie' of met 100 percent zekerheid de locatie identificeren van waar een cyberaanval komt, is zeer moeilijk. Een aanval gedirigeerd vanuit een bepaalde locatie, kan immers via een gehackte, of door een virus geïnfecteerde computer vanuit een andere locatie uitgevoerd worden. Vanuit die optiek kan ik u geen cijfers bezorgen m.b.t. eventuele cyberaanvallen vanuit China op Vlaamse overheidsnetwerken.

3. Het komt, gegeven mijn bevoegdheden, niet aan mij toe om hieromtrent een dergelijk initiatief te nemen. Uiteraard zijn er binnen de administratie contacten met de bevoegde federale instanties zoals het Belgische Centrum voor Cybersecurity (CCB), dat zoals de Vlaamse overheid deel uit maakt van de Cybersecurity Coalitie.
4. Het in kaart brengen van de cyberdreigingen in Vlaanderen (breder dan de gemeenschappelijke ICT-dienstverlening van de Vlaamse overheid) valt buiten mijn bevoegdheid.