Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

428

Vragen van de leden **Van Helvert**, **Van der Molen** en **Van den Berg** (allen CDA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties en van Buitenlandse Zaken over *het bericht dat China wereldwijd 2,4 miljoen sleutelfiguren volgt* (ingezonden 16 september 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Buitenlandse Zaken (ontvangen 12 oktober 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 269.

Vraag 1
Kent u het bericht «China volgt wereldwijd 2,4 miljoen sleutelfiguren»?[1]

Antwoord 1
Ja.

Vraag 2
Heeft u de informatie uit de gelekte databank in kunnen zien en/of informatie ontvangen over de databank? Zo ja, staan er ook Nederlanders in de databank? Zullen de Nederlanders die door Zhenhua Data zijn aangemerkt als «sleutelfiguur» en vanuit China in de gaten worden gehouden, hierover worden geïnformeerd?

Antwoord 2
Ik ben geïnformeerd over de databank. Vanwege de bijzondere verantwoordelijkheid van de rijksoverheid voor het stelsel bewaken en beveiligen heb ik laten onderzoeken of personen die een bijzondere functie hebben in de democratische rechtsorde in het databestand voorkomen. Dit blijkt het geval. Betreffende personen zijn hierover geïnformeerd.

Vraag 3
Kunt u aangeven of het verzamelen van data over Nederlandse «sleutelfiguren» de aanhoudende aandacht heeft van onze inlichtingendiensten?

[1] Nos.nl, 14 september 2020, «China volgt wereldwijd 2,4 miljoen sleutelfiguren» (https://nos.nl/artikel/2348184-china-volgt-wereldwijd-2-4-miljoen-sleutelfiguren.html)

ah-tk-20202021-428
ISSN 0921 - 7398
's-Gravenhage 2020

Antwoord 3
Deze mediaberichten passen in het beeld van de dreiging die uitgaat van statelijke actoren, zoals ook blijkt uit onder andere cybersecuritybeelden van de afgelopen jaren en de jaarverslagen van de inlichtingen- en veiligheidsdiensten.
Hiervoor is inderdaad aanhoudende aandacht.

Vraag 4
Met welke intenties denkt u dat een Chinees bedrijf op grote schaal persoonsgegevens en potentieel compromitterende informatie van miljoenen mensen wereldwijd verzamelt?

Antwoord 4
Er zijn statelijke actoren die op grote schaal persoonsgegevens verzamelen, zowel uit open bronnen, zoals op basis van contacten die iemand onderhoudt op sociale media, als uit niet-openbare bronnen, bijvoorbeeld door het hacken van de systemen van hotelketens, telecombedrijven en medische instellingen.
De afgelopen jaren hebben de inlichtingen- en veiligheidsdiensten meermaals in jaarverslagen gemeld dat statelijke actoren gegevens verzamelen die voor hen op velerlei manieren van nut kunnen zijn, waaronder voor doeleinden die andere personen, organisaties of landen schaden. Voorbeelden hiervan zijn politieke en economische spionage, beïnvloeding van diaspora of het uitvoeren van digitale aanvallen (bijvoorbeeld phishing). Daarbij kan (vertrouwelijke) informatie van bijvoorbeeld ambtenaren, wetenschappers, topfunctionarissen en journalisten gericht worden gebruikt.

Vraag 5
Kunt u bevestigen dat de Chinese Volkspartij en het Chinese leger klant zijn van het Chinese techbedrijf Zhenhua Data? Heeft u indicaties dat Chinese veiligheidsdiensten opdracht gaven voor de deze operatie?

Antwoord 5
In de media wordt melding gemaakt van het feit dat Zhenhua Data de Chinese Communistische Partij en het Volksbevrijdingsleger als voornaamste klanten zou hebben. Het kabinet kan dit niet bevestigen. Op dit moment heeft het kabinet geen indicaties dat de Chinese veiligheidsdiensten opdracht hebben gegeven voor het verzamelen van data en het aanleggen van een database door Zhenhua Data.

Vraag 6
Kan deze gedetailleerde Chinese informatievergaringsoperatie worden beschouwd als een poging van de Chinese regering om ook personen buiten China te vangen in een sociaal kredietsysteem? Wat zegt dit alles over de intenties van China op het wereldtoneel?

Antwoord 6
Zoals aangegeven in het antwoord op vragen 3 en 4 passen de mediaberichten in het beeld van de dreiging die uitgaat van statelijke actoren, zoals ook blijkt uit onder andere cybersecuritybeelden van de afgelopen jaren, de jaarverslagen van de inlichtingen- en veiligheidsdiensten. Voorbeelden hiervan zijn politieke en economische spionage, beïnvloeding van diaspora of het uitvoeren van digitale aanvallen (bijvoorbeeld phishing). Daarbij kan (vertrouwelijke) informatie van bijvoorbeeld ambtenaren, wetenschappers, topfunctionarissen en journalisten gericht worden gebruikt. Het kabinet heeft geen aanwijzingen dat het databestand van het bedrijf Zhenhua deel uitmaakt van het Chinese sociaalkredietsysteem.

Vraag 7
Welke acties bent u van plan te nemen naar aanleiding van deze bevindingen?

Antwoord 7
Weerbaarheid tegen statelijke dreigingen is van groot belang. Het kabinet zet zich, zoals gemeld in de Kamerbrief tegengaan statelijke dreigingen[2], in voor verhoging van de weerbaarheid op het terrein van het tegengaan van ongewenste buitenlandse inmenging via diaspora, voor het beschermen van democratische instituties en processen en voor het versterken van de economische veiligheid. Daarnaast wordt er via de uitvoering van de Nederlandse Cybersecurity Agenda structureel ingezet op het verhogen van de digitale weerbaarheid van Nederland. Eerdergenoemde berichtgeving toont aan dat bewustwording bij personen en organisaties voor digitale veiligheid een essentieel onderdeel vormt van deze aanpak. Het kabinet zet zich daarom ook onverminderd in voor onder andere tijdige detectie en optimalisering van cyber-weerbaarheid van de Nederlandse samenleving en specifiek ten aanzien van instellingen die dergelijke data verzamelen.
Naar aanleiding van de genoemde berichtgeving is een infosheet «Beschermen Persoonsgegevens» opgesteld om mensen te informeren over de risico's van digitalisering en handvatten te bieden hoe online persoonsgegevens te beschermen. Dit infosheet is verspreid naar de relevante organisaties en te vinden op de website van de NCTV.

Vraag 8
Wat betekent deze schokkende onthulling voor de toekomstige positie van Chinese leveranciers van telecombedrijven op de Nederlandse markt?

Antwoord 8
Op 1 juli 2019 heeft het kabinet aanvullende beschermingsmaatregelen aangekondigd voor de veiligheid en integriteit van de telecomnetwerken en -diensten[3]. Deze maatregelen zijn genomen op basis van een risicoanalyse van de Task Force Economische Veiligheid met medewerking van de drie grote telecomaanbieders. Het kabinet kiest hierbij voor een landenneutrale en daarmee toekomstbestendige aanpak, dat wil zeggen, een aanpak op basis van objectieve criteria die mee kan bewegen met een veranderend dreigingsbeeld en onvoorziene technologische en marktontwikkelingen.

[2] Kamerstukken II 2018–2019, 30 821, nr. 72
[3] Kamerstukken II 2018–2019, 30 821, nr. 92