Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

3100

Vragen van het lid **Belhaj** (D66) aan de Staatssecretaris van Defensie over *het bericht «Bellingcat: Bierapp Untappd kan gebruikt worden om militairen te volgen»* (ingezonden 25 mei 2020).

Antwoord van Minister **Bijleveld-Schouten** (Defensie) (ontvangen 10 juni 2020).

Vraag 1
Hebt u kennisgenomen van het artikel «Bellingcat Bierapp Untappd kan gebruikt worden om militairen te volgen»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de zorgen dat het uitlekken van persoonsgegevens van Nederlandse militairen de veiligheid van deze militairen en de nationale veiligheid in het geding kan brengen?

Antwoord 2
Het uitlekken van persoonsgegevens van Nederlandse militairen moet zo veel mogelijk worden voorkomen. Het gebruik van sociale media en *smart devices* is wijd verspreid en diep geworteld. Informatiedeling hoort bij de hedendaagse maatschappij. Voorkomen moet worden dat dit risico's oplevert voor de militair, zijn of haar gezin en lopende operaties. Bewustzijn en collegiale controle zijn van essentieel belang om er voor te zorgen dat deze risico's worden beperkt. Defensie besteedt daarom voortdurend aandacht aan het verhogen van het beveiligingsbewustzijn, ook als het gaat om het zorgvuldig omgaan met persoonsgegevens. Defensiemedewerkers worden regelmatig gewezen op de risico's van het delen van persoonsgegevens waarbij een relatie met Defensie kan worden gelegd.

[1] https://www.nu.nl/tech/6052165/bellingcat-bierapp-untappd-kan-gebruikt-worden-om-militairen-te-volgen.html

ah-tk-20192020-3100
ISSN 0921 - 7398
's-Gravenhage 2020

Vraag 3
Daar waar in 2018 bekend werd dat het gebruik van sportapps of telefoons van militairen ook privacyrisico's met zich meebrach, zijn deze risico's inmiddels verholpen?

Antwoord 3
Alle apps en alle sociale media zijn in potentie een risico. Defensiemedewerkers worden regelmatig gewezen op de risico's van het delen van persoonsgegevens waarbij een relatie met Defensie kan worden gelegd. Daarnaast zijn er handreikingen over hoe instellingen op de juiste manier worden ingesteld zodat risico's van apps beperkt worden. Zo wordt er al speciaal gewezen op de gevaren van het «inchecken» op Defensielocaties en locatievoorzieningen. Ook wordt per missie gekeken wat de dreiging is en wat dat betekent voor het gebruik van apps en sociale media door militairen op missie. Zo kunnen er strengere maatregelen gelden in specifieke missiegebieden dan op andere locaties.

Vraag 4
Vallen de regels voor de Bierapp Untappd onder dezelfde, destijds opgestelde, regels naar aanleiding van het incident in 2018?

Antwoord 4
Ja. Naar aanleiding van de gebeurtenissen in 2018 is het Defensie Beveiligingsbeleid aangepast. Dit beleid is nog steeds van kracht. Eén van de regels is bijvoorbeeld dat privé *devices* op missie alleen in rustgebieden (legering en kantine) mogen worden gebruikt. Het gedrag van de medewerkers zelf is bepalend. Bewustzijn en collegiale controle zijn daarom van essentieel belang om ervoor te zorgen dat de risico's verder worden beperkt. Het zorgvuldig omgaan met privacy-instellingen bij het gebruik van apps is een constant punt van aandacht. De individuele medewerker is en blijft mede verantwoordelijk voor de collectieve veiligheid.

Vraag 5
Kunt u de Kamer bevestigen dat Defensie voldoende maatregelen neemt om deze problemen op te lossen?

Antwoord 5
Defensie is zich bewust van de kwetsbaarheden die *smart devices* met zich meebrengen. Nieuwe technieken vragen continu om een risicobeoordeling. Defensiemedewerkers worden regelmatig geïnformeerd over de gevaren en het gebruik hiervan. Per missie gelden aanvullende, specifieke regels. Door middel van maatwerk worden de risico's van apps en sociale media zo veel mogelijk geminimaliseerd.