

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

2160

Vragen van de leden **Nordkamp** en **Kathmann** (beiden GroenLinks-PvdA) aan de Minister van Defensie en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de bescherming van persoonsgegevens van militairen op apps* (ingezonden 24 maart 2025)

Antwoord van Staatssecretaris **Tuinman** (Defensie) (ontvangen 9 mei 2025).

Vraag 1

Bent u bekend met het bericht «Persoonsgegevens honderden militairen zichtbaar via sportapp Strava»?¹

Antwoord 1

Ja.

Vraag 2

Hoe lang bent u al op de hoogte dat apps zoals Strava de veiligheid van Nederlandse militairen in gevaar brengen?

Antwoord 2

In 2018 heeft Defensie haar beleid voor het gebruik van dergelijke applicaties aangescherpt nadat een bedrijf een wereldwijde *heatmap* publiceerde waarop ook activiteiten van Defensie zichtbaar waren. Hierop waren onder meer de locaties van militaire bases zichtbaar.

Vraag 3

Met hoeveel zekerheid kunt u zeggen dat er al sprake is van het combineren van openbare of gelekte informatie over militairen door kwaadwillenden? Op welke schaal vindt dit plaats?

¹ Omroep Gelderland, 19 maart 2025, Persoonsgegevens honderden militairen zichtbaar via sportapp Strava, (<https://www.gld.nl/nieuws/8285161/persoonsgegevens-honderden-militairen-zichtbaar-via-sportapp-strava>)

Antwoord 3

In brede zin is het aannemelijk dat locatiegegevens van militairen in handen zijn van andere partijen. Uit het Dreigingsbeeld Statelijke Actoren² van november 2022 (bijlage bij Kamerbrief 4341330) blijkt dat statelijke actoren, waaronder China, op grote schaal persoonsgegevens verzamelen. Deze gegevens komen zowel uit open bronnen (zoals sociale media) als gesloten bronnen (door hacks). Ook in Nederland is deze vergaring van informatie waargenomen. Dat is een zorgelijke ontwikkeling waar ik me bewust van ben. Daarom zet ik me in om het cyberbewustzijn en de cyberveiligheid te vergroten.

Vraag 4

Deelt u de mening dat privacybescherming van militairen in direct verband staat met hun persoonlijke veiligheid en de nationale veiligheid?

Antwoord 4

Ja. Militairen vormen een doelgroep waarvan privégegevens en locatiegegevens waardevol zijn voor (vooral) statelijke actoren. Het onbewust delen van deze gegevens door militairen in een operatiegebied kan risico's opleveren voor zowel de eigen veiligheid, als de operationele veiligheid. Daarom worden militairen die op uitzending gaan vooraf en tijdens de missie gewezen op de risico's daarvan. Mede vanwege deze risico's zijn vele applicaties, waaronder fitness-applicaties, niet toegestaan op defensieapparatuur. De applicaties kunnen echter wel op de privéapparatuur worden geïnstalleerd, hetgeen door Defensie niet kan worden verboden. Het gebruik van privéapparatuur is in sommige situaties dan ook aan restricties onderhevig. Defensie besteedt verder veel aandacht aan de bewustwording van de risico's.

Vraag 5

Deelt u de mening dat, vanuit het veiligheidsperspectief voor Nederlandse militairen, maximale privacybescherming op online platforms noodzakelijk is?

Antwoord 5

Ja. Defensie heeft echter geen zeggenschap over privéapparatuur en het privégebruik van het Internet. Defensie richt zich hierbij dus vooral op advisering en voorlichting.

Vraag 6

Op welke manier doet u aan advisering en voorlichting voor militairen over online veiligheid? Welke regels gelden er voor zowel werk- als privételefoongebruik? Verschilt dit tussen militairen in Nederland en uitgezonden militairen?

Antwoord 6

Defensie informeert en traint militairen actief over (cyber)veiligheid van het gebruik van mobiele apparatuur. Elke militair doorloopt jaarlijks een training inzake militaire basisvaardigheden (MBV) en sinds twee jaar is aan die training een module cyberveiligheid toegevoegd.

Daarnaast is een Handboek Cyberveilig Gedrag uitgebracht, dat regels en aanbevelingen uiteen zet voor het gebruik van zowel privé als defensietelefoons. Een speciale cyberapplicatie is eveneens geïntroduceerd om militairen te informeren over cyberveiligheid. Elke defensiemedewerker heeft toegang tot deze applicatie.

Defensie heeft controle over de werktelefoons en kan daardoor bepaalde applicaties weren. Voor privételefoons is deze controle niet mogelijk, tenzij een militair op missie wordt gestuurd. In dat geval worden militairen geïnformeerd over de specifieke regels en risico's van telefoongebruik in het operatiegebied. Bovendien kunnen er tijdens een inzet aanvullende beveiligingseisen en restricties gelden voor zowel defensie- als privéapparatuur, om de veiligheid te waarborgen.

² *Dreigingsbeeld Statelijke actoren 2. (28-11-2022)*. Publicatie Nationaal Coördinator Terrorisme-
bestrijding en Veiligheid. [https://www.nctv.nl/documenten/publicaties/2022/11/28/
dreigingsbeeld-statelijke-actoren-2](https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2)

Vraag 7

Bent u bereid tot meer dwingende maatregelen, zoals het verbieden van sportapps en andere apps die de privacy van militairen schaden op militair terrein? Zo nee, waarom niet?

Antwoord 7

Op Defensieapparatuur zijn reeds bepaalde applicaties verboden waardoor deze niet geïnstalleerd en gebruikt kunnen worden. Om de digitale veiligheid van militairen te blijven waarborgen, monitort en analyseert Defensie continu de nieuwste technologische ontwikkelingen om eventuele risico's te identificeren. Wanneer nodig worden mitigerende maatregelen getroffen en worden de veiligheidsprotocollen bijgesteld en verbeterd.

Op apparaten die niet beheerd worden door Defensie is het stellen van dwingende maatregelen niet mogelijk. Zoals aangegeven werkt Defensie via training en opleiding aan het veiligheidsbewustzijn van haar medewerkers.

Vraag 8

Welke acties heeft u ondernomen om de online veiligheid van militairen beter te beschermen, ook na eerdere berichtgeving en Kamervragen over de privacygevolgen van datingapps en sportapps?^{3, 4}

Antwoord 8

Naar aanleiding van de eerdere berichtgeving en Kamervragen rondom het gebruik van dergelijke applicaties (2018), is het beleid aangescherpt. Bepaalde applicaties kunnen niet worden geïnstalleerd op defensieapparatuur. Voor de overige maatregelen verwijs ik naar de antwoorden op vragen 6 en 7.

Vraag 9

Hebben de acties die u heeft genomen om de online veiligheid van militairen beter te beschermen effect gehad? Kunt u dit onderbouwen?

Antwoord 9

Kenmerkend van het nemen van maatregelen ter verhoging van de informatiebeveiliging en de cybersecurity is, dat het lastig is om de effectiviteit te bepalen. Het is daarom van groot belang om constant alert te zijn op bestaande en nieuwe kwetsbaarheden en dreigingen, en op basis van risicoanalyses gepaste maatregelen te treffen.

Vraag 10

Bent u bekend met het onderzoek van de KU Leuven uit 2022, waaruit blijkt dat eerdere oplossingen van Strava vooral tot schijnveiligheid leiden?⁵

Antwoord 10

Ja. Het onderzoek onderstreept het belang van de door Defensie getroffen maatregelen.

Vraag 11

Welke technische mogelijkheden ziet u om de veiligheid van militairen beter te beschermen bij het gebruik van sportapps, datingapps of andere apps die hun data verzamelen?

Antwoord 11

Indien wordt gesignaleerd dat een bepaalde applicatie een risico vormt voor Defensie, wordt beoordeeld of deze applicatie beschikbaar gesteld kan worden. Op defensieapparatuur zijn maatregelen getroffen dat, indien een applicatie niet toegestaan is en de applicatie toch wordt geïnstalleerd, de

³ Follow the Money, 16 december 2024, Tinderende militairen tonen nogmaals aan: privacy is niet de vijand van veiligheid (<https://www.ftm.nl/artikelen/analyse-privacy-is-niet-de-vijand-van-veiligheid?share=JWekA1NvF6dXXn6keJ5CcS%2BLgxmAzW2yz2y036xLyaLZPys9Ys4CTs8Kla329l%3D>)

⁴ Tweede Kamer, 30 januari 2018, D66 vraagt naar traceerbaarheid militairen door apps, (https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/d66-vraagt-naar-traceerbaarheid-militairen-door)

⁵ Dhondt et. al, 7 november 2022, A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks, (<https://dl.acm.org/doi/10.1145/3548606.3560616>)

defensieomgeving wordt geblokkeerd. Privéapparatuur is niet in beheer van Defensie en door Defensie kan dan ook technisch niet worden afgedwongen welke applicaties worden gebruikt en welke websites worden bezocht. Om risico's op dit gebied toch te mitigeren, besteedt Defensie aandacht aan het veiligheidsbewustzijn van de defensiemedewerkers.

Vraag 12

Is het mogelijk om te achterhalen, al dan niet in overleg met Strava, of de openbare profielen van militairen mogelijk door kwaadwillenden zijn bekeken?

Antwoord 12

Juridisch gezien is dit niet mogelijk omdat Defensie geen grond heeft om deze persoonsgegevens op te vragen. De gegevens zijn vanaf privéapparatuur gegenereerd en volgens de AVG niet in te zien door Defensie. Daarnaast is het praktisch onuitvoerbaar om logbestanden van bezoeken op openbare profielen van militairen te onderzoeken op een bezichtiging van dat profiel door een mogelijk kwaadwillende actor.

Vraag 13

In hoeverre zijn militairen die een gesloten account hebben echt veilig? Welke derde partijen hebben toegang tot de informatie die Strava verzamelt, ook als een account gesloten is? Waaruit blijkt dit?

Antwoord 13

Defensie beschikt niet over deze gegevens. De applicatie mag niet op defensieapparatuur worden geïnstalleerd. Indien de militair een dergelijke applicatie toch wil installeren, volgt een waarschuwing om de applicatie te verwijderen. Indien dat niet gebeurt, zal de telefoon voor de defensieomgeving worden geblokkeerd.

Vraag 14

Ziet u gezien de onvoorspelbare geopolitieke situatie aanleiding om het beleid rondom het gebruik van Amerikaanse apps door militairen te heroverwegen en aan te scherpen?

Antwoord 14

De onvoorspelbare geopolitieke situatie biedt aanleiding om scherp te zijn op alle factoren die een potentieel risico vormen voor nationale, operationele en persoonlijke veiligheid. Dit beperkt zich niet tot apps afkomstig uit landen met een offensief cyberprogramma. De maatregelen die nu gelden voor gebruik van externe apps blijven van kracht. Indien blijkt dat een app een risico vormt voor Defensie dan kan de app worden geweerd. Dit is niet gebonden aan een specifiek land.

Vraag 15

Kunt u deze vragen afzonderlijk en uiterlijk drie dagen vóór het commissiedebat «Hybride dreigingen en maatschappelijke weerbaarheid» beantwoorden?

Antwoord 15

Nee, zoals gemeld in het uitstelbericht welke verzonden is op 8 april⁶, is in verband met de omvang en complexiteit van de vragen dit niet mogelijk gebleken.

⁶ MINDEF20250014326 – Uitstel beantwoording schriftelijke vragen van de leden Van der Werf (D66), Boswijk (CDA), Nordkamp en Kathmann (beide GL/PvdA) over het traceren van militairen met apps