



Ministerie van Defensie

Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie

MINDEF20250015738

*Bij beantwoording, datum,
onze referentie en
onderwerp vermelden.*

> Retouradres Postbus 20701 2500 ES Den Haag
de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

Datum 9 mei 2025
Betreft Beantwoording vragen traceren militairen via fitness apps

Geachte voorzitter,

Hierbij bied ik, mede namens de Minister van Defensie, de antwoorden aan op de schriftelijke vragen gesteld door de leden Van der Werf (D66) & Boswijk (CDA) over 'Het traceren van militairen via fitness-apps'. Deze vragen werden ingezonden op 20 maart 2025 met kenmerk 2025Z05222.

Daarnaast bied ik hierbij ook, mede namens de staatssecretaris van Binnenlandse zaken en Koninkrijksrelaties, de antwoorden aan op de schriftelijke vragen gesteld door Nordkamp en Kathmann (beiden Groenlinks-PvdA) over 'De bescherming van persoonsgegevens van militairen op apps'. Deze vragen werden ingezonden op 24 maart 2025 met kenmerk 2025Z06467.

Hoogachtend,

DE STAATSSECRETARIS VAN DEFENSIE

Gijs Tuinman

Kamervragen 2025Z05222

(ingezonden 20 maart 2025)

Vragen van het lid Van der Werf (D66) en Boswijk (CDA) aan de minister van Defensie over het traceren van militairen via fitness-apps.

1. Bent u bekend met het bericht van de NOS waarin wordt gesteld dat ruim duizend Nederlandse militairen te traceren zijn via de fitness-app Strava? [1]

Ja.

2. Hoe beoordeelt u het risico dat operationele veiligheid en persoonlijke veiligheid van Nederlandse militairen in gevaar komt door het ongewenst delen van locatiegegevens?

De operationele en persoonlijke veiligheid van Nederlandse militairen is voor mij van groot belang. Een situatie waarin militairen zijn te traceren door het gebruik van een applicatie is dan ook onacceptabel. Om dit risico te mitigeren, is de betreffende applicatie, net als vergelijkbare fitness-applicaties, niet toegestaan op defensieapparaten. Wanneer de militair een dergelijke applicatie toch wil installeren, volgt een waarschuwing om de app te verwijderen. Indien dat niet gebeurt zal de telefoon voor de defensieomgeving worden geblokkeerd.

Daarnaast worden militairen ook voorgelicht over cyberveilig-gedrag, waaronder het gebruik van deze applicaties op de privé-telefoon. Dit gebeurt onder andere tijdens de jaarlijks verplichte toetsing van de militaire basisvaardigheden. Om de operationele en persoonlijke veiligheid van militairen te beschermen, worden zij vooraf en tijdens een oefening of missie gewezen op de risico's van het delen van locatiegegevens. In sommige gevallen verbiedt Defensie het meenemen van een smartphone op oefeningen of missies. De aard, context en locatie van de missie bepaalt of deze regelgeving van toepassing is.

3. Welke maatregelen treft Defensie momenteel om veilig te stellen dat militairen op hun privételefoon gewoon gebruik kunnen maken van dergelijke sportapps?

Defensie voert niet het beheer over de privé-apparaten van militairen. Defensie wijst militairen en burgers via diverse interne cyber awareness maatregelen op de risico's die men loopt door op defensie- en privé-apparaten applicaties te gebruiken die gebruik maken van locatiegegevens.

4. Bent u van plan aanvullende maatregelen te nemen om de digitale veiligheid van militairen beter te beschermen? Zo ja, welke? Zo nee, waarom niet?

De digitale veiligheid van militairen wordt op devices die in beheer zijn van Defensie goed beschermd, dit mede door het verbieden van dergelijke fitnessapps. Om militairen toch de gelegenheid te bieden sportprestaties te registreren heeft Defensie een alternatieve fitness-applicatie beschikbaar gesteld. Deze data wordt zo op een veilige manier verwerkt.

Bovendien heeft Defensie reeds verschillende maatregelen genomen om de digitale veiligheid van militairen te bevorderen. Zo volgt elke militair jaarlijks een module over cyberveiligheid tijdens de training militaire basisvaardigheden. Daarnaast is er een handboek "Cyberveilig Gedrag" uitgebracht, dat voor alle defensiemedewerkers toegankelijk is en hen informeert over digitale veiligheid. Defensie blijft continu de digitale veiligheid van militairen monitoren en analyseert de nieuwste technologische ontwikkelingen om eventuele risico's te identificeren. Wanneer nodig worden mitigerende maatregelen getroffen en worden de veiligheidsprotocollen bijgesteld en verbeterd om de digitale veiligheid van militairen optimaal te waarborgen.

5. Worden Nederlandse militairen actief geïnformeerd en getraind over de risico's van fitness-apps en andere applicaties die locatiegegevens kunnen delen? Zo ja, hoe en hoe vaak? Zo nee, waarom niet?

Ja, Nederlandse militairen worden actief geïnformeerd en getraind over de risico's van fitness-apps en andere applicaties die locatiegegevens kunnen delen. Elke militair doorloopt jaarlijks een training inzake militaire basisvaardigheden (MBV), waarbij een module 'cyberveiligheid' is toegevoegd. Via deze module worden de digitale risico's van digitale applicaties behandeld.

Daarnaast is begin dit jaar voor alle defensiemedewerkers een Handboek Cyberveilig Gedrag uitgebracht, waarin deze risico's nader worden toegelicht. Dit handboek is via het Intranet van Defensie breed bekend gesteld. Bovendien is in dezelfde periode een speciale cyberapplicatie geïntroduceerd, die alle defensiemedewerkers via hun defensieapparaten tot hun beschikking hebben. In deze appli-

catie zijn de trainingsmodules van de MBV en het Handboek Cyberveilig Gedrag integraal meegenomen.

6. Zijn er gevallen bekend waarbij locatiegegevens van Nederlandse militairen in verkeerde handen zijn gevallen of mogelijk misbruikt zijn? Zo ja, welke consequenties heeft dat gehad?

In brede zin is het aannemelijk dat locatiegegevens van militairen in handen zijn van andere partijen. Uit het Dreigingsbeeld Statelijke Actoren¹ 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.

7. Heeft Defensie contact opgenomen met Strava of andere fitness-apps om maatregelen te nemen, zoals het standaard uitsluiten van militaire locaties?

Nee. Defensie heeft geen contact opgenomen met Strava of andere fitness-apps om maatregelen te nemen, zoals het standaard uitsluiten van militaire locaties. Defensie hanteert een eigen stringent applicatiebeleid dat de veiligheid en beveiliging van onze medewerkers en locaties waarborgt. Onderdeel hiervan is dat deze applicatie niet gebruikt kan worden op apparaten van Defensie.

8. Wat kunnen andere overheidsorganisaties leren van deze situatie met betrekking tot digitale veiligheid en het gebruik van commerciële applicaties door overheidsmedewerkers?

Interdepartementaal vindt regulier overleg plaats tussen de Chief Information Security Officers (CISO's). Een vrijwel continu aandachtspunt zijn de risico's van het gebruik van applicaties op overheidsapparatuur. Op basis van het appbeleid zijn apps van landen met een offensief cyberprogramma uitgesloten op zakelijke apparaten². Het is goed om constant alert te blijven op de gevolgen van het gebruik van applicaties, ook als deze niet vallen onder het Rijksbrede appbeleid rondom applicaties uit landen met een offensief cyberprogramma. Op dit moment wordt bij de rijksoverheid het appbeleid geïmplementeerd waarbij alleen zakelijke applicaties zijn toegestaan op zakelijke apparaten van hoog risico functionarissen³. Vanwege de hoge risico's voor militairen op defensieterrain en bij inzet worden specifieke applicaties verboden op defensiedevices en het gebruik van civiele apparatuur afgeraden.

9. Welke stappen neemt Defensie om de digitale weerbaarheid van de krijgsmacht structureel te verbeteren, specifiek met betrekking tot het gebruik van commerciële apps die data verzamelen?

Defensie neemt verschillende stappen om de digitale weerbaarheid van de krijgsmacht te verbeteren, met name met betrekking tot het gebruik van commerciële apps die data verzamelen. Defensie volgt de technologische ontwikkelingen nauwgezet en draagt zorg voor het vergroten van de bewustwording van defensiepersoneel omtrent cybersecurity.

Militairen worden extra geïnformeerd over de risico's van commerciële apps bij oefeningen en missies. Daarbij is het meebrengen van smartphones tijdens specifieke missies niet toegestaan. Deze maatregelen helpen om de digitale veiligheid van de krijgsmacht te waarborgen.

Defensie blijft continu de digitale veiligheid van militairen monitoren en analyseert de ontwikkelingen rondom nieuwe applicaties en technologieën om eventuele risico's te identificeren. Wanneer nodig worden mitigerende maatregelen getroffen, zoals het direct blokkeren van apps die een risico vormen. Op deze manier kan Defensie snel en effectief reageren op nieuwe bedreigingen en ervoor zorgen dat de digitale veiligheid gewaarborgd is.

10. Op welke wijze worden militaire veiligheidsprotocollen aangepast naar aanleiding van technologische ontwikkelingen zoals deze?

¹ Dreigingsbeeld Statelijke actoren 2. (28-11-2022). Publicatie Nationaal Coördinator Terrorismebestrijding en Veiligheid. <https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2>

² Kamerstukken 26 643, nr. 1087

³ Kamerstukken 26 643, nr. 1197

Technologische ontwikkelingen maken het noodzakelijk om continu de veiligheidsprotocollen te blijven beoordelen en te verbeteren. Dit gebeurt door het maken van risicoanalyses, op basis waarvan eventuele mitigerende maatregelen worden getroffen.

11. Welke stappen zijn gezet na eerdere berichtgeving over de risico's van datingapps en de eerdere berichten over sportapps? [2]

Naar aanleiding van verdere berichtgeving heeft Defensie het beleid rondom het gebruik van dergelijke applicaties aangescherpt. Omdat het werk van militairen fysiek is wil Defensie sporten stimuleren. Daarom heeft Defensie de fitness-app DTCS ontwikkeld, zodat militairen hun sportprestaties kunnen registreren. Deze applicatie is op de diensttelefoon te installeren en te gebruiken. Daarnaast wordt het defensiepersoneel geïnformeerd over de risico's van commerciële apps door middel van trainingen, een handboek en een speciale cyberapplicatie.

[1] NOS, 19 maart 2025, Ruim duizend militairen te traceren via Strava: 'Vijand kan data misbruiken', (<https://nos.nl/artikel/2560278-ruim-duizend-militairen-te-traceren-via-strava-vijand-kan-data-misbruiken>)

[2] NOS, 14 december 2024, 'Militairen op datingapp Tinder gevaar voor nationale veiligheid', (<https://nos.nl/artikel/2548255-militairen-op-datingapp-tinder-gevaar-voor-nationale-veiligheid>)

2025Z05467

(ingezonden 24 maart 2025)

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

1. Bent u bekend met het bericht ‘Persoonsgegevens honderden militairen zichtbaar via sportapp Strava’? [1]

Ja.

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

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.

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?

In brede zin is het aannemelijk dat locatiegegevens van militairen in handen zijn van andere partijen. Uit het Dreigingsbeeld Statelijke Actoren⁴ 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.

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

Ja. Militairen vormen een doelgroep waarvan privé-gegevens 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.

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

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

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

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

⁴ Dreigingsbeeld Statelijke actoren 2. (28-11-2022). Publicatie Nationaal Coördinator Terrorismebestrijding en Veiligheid. <https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2>

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.

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?

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.

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? [2] [3]

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.

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

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.

10. Bent u bekend met het onderzoek van de KU Leuven uit 2022, waaruit blijkt dat eerdere oplossingen van Strava vooral tot schijnveiligheid leiden? [4]

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

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?

Indien wordt signaleerd 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 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.

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?

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.

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?

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.

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?

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.

15. Kunt u deze vragen afzonderlijk en uiterlijk drie dagen vóór het commissiedebat “Hybride dreigingen en maatschappelijke weerbaarheid” beantwoorden?

Nee, zoals gemeld in het uitstelbericht welke verzonden is op 8 april^[1], is in verband met de omvang en complexiteit van de vragen dit niet mogelijk gebleken.

[1] 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

[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>)

[2] 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%2BLgxmAzW2yz2y036xLyaLZPys9Ys4CTs8Kla329I%3D>)

[3] 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)

[4] 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>)