Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

2134

Vragen van het lid **Van der Werf** (D66) en **Boswijk** (CDA) aan de Minister van Defensie over *het traceren van militairen via fitness-apps* (ingezonden 20 maart 2025).

Antwoord van Staatssecretaris **Tuinman** (Defensie) (ontvangen 9 mei 2025).
Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 1885.

Vraag 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]

Antwoord 1
Ja.

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

Antwoord 2
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 privételefoon. 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

[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)

ah-tk-20242025-2134
ISSN 0921 - 7398
's-Gravenhage 2025

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.

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

Antwoord 3
Defensie voert niet het beheer over de privéapparaten van militairen. Defensie wijst militairen en burgers via diverse interne cyber awareness maatregelen op de risico's die men loopt door op defensie- en privéapparaten applicaties te gebruiken die gebruik maken van locatiegegevens.

Vraag 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?

Antwoord 4
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.

Vraag 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?

Antwoord 5
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 applicatie zijn de trainingsmodules van de MBV en het Handboek Cyberveilig Gedrag integraal meegenomen.

Vraag 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?

Antwoord 6
In brede zin is het aannemelijk dat locatiegegevens van militairen in handen zijn van andere partijen. Uit het Dreigingsbeeld Statelijke Actoren[2] 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 7
Heeft Defensie contact opgenomen met Strava of andere fitness-apps om maatregelen te nemen, zoals het standaard uitsluiten van militaire locaties?

Antwoord 7
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.

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

Antwoord 8
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 cyberpro-gramma uitgesloten op zakelijke apparaten[3].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 functionarissen[4]. Vanwege de hoge risico's voor militairen op defensieterreinen en bij inzet worden specifieke applicaties verboden op defensiedevices en het gebruik van civiele apparatuur afgeraden.

Vraag 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?

Antwoord 9
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

---

[2] *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
[3] Kamerstukken 26 643, nr. 1087
[4] Kamerstukken 26 643, nr. 1197

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.

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

Antwoord 10
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.

Vraag 11
Welke stappen zijn gezet na eerdere berichtgeving over de risico's van datingapps en de eerdere berichten over sportapps?[5]

Antwoord 11
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.

[5] 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)