Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Ons kenmerk
a4b2ce75-or1-1.3

Uw kenmerk
2026Z22881

Bijlagen
0

Datum 12 november 2026
Betreft Beantwoording Kamervragen lid Van Leijen (D66) over spionagerisico's slimme voertuigen

Hierbij bieden wij u de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid Van Leijen (D66) over de AIVD-publicatie 'De moderne auto als mogelijke spion'. Deze vragen werden ingezonden op 23 oktober 2026 met kenmerk 2026Z22881.

De minister van Binnenlandse Zaken
en Koninkrijksrelaties,

Pieter Heerma

De minister van Infrastructuur
en Waterstaat,

V.P.G. Karremans

Vraag 1
Bent u bekend met de publicatie 'De moderne auto als mogelijke spion. Digitale dreigingen in slimme voertuigen' van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) van 30 september 2026?[1]

Antwoord 1
Ja.

Vraag 2
Zijn er in Nederland gevallen bekend waarin microfoons of camera's in voertuigen op afstand zijn ingeschakeld of waarin dat is geprobeerd en bent u bereid de Kamer hierover zo nodig vertrouwelijk te informeren?

Antwoord 2
De publicatie van de AIVD geeft een overzicht van de voorstelbare spionagerisico's die gepaard kunnen gaan met het gebruik van moderne voertuigen, inclusief adviezen hoe met dergelijke risico's om kan worden gegaan. In deze publicatie roept de AIVD op om bewust om te gaan met dergelijke spionagerisico's. De AIVD doet in het openbaar geen uitspraken over eventuele onderkende gevallen of incidenten van spionage in of door middel van het gebruik van voertuigen.

Vraag 3
Deelt u, gelet op de vaststelling van de AIVD dat risico's via gps, de telematicamodule en laadpalen "niet te voorkomen [zijn] met techniek of door gedrag", de opvatting dat deze risico's niet bij de individuele gebruiker kunnen worden neergelegd maar om regelgeving vragen?

Antwoord 3
Digitale producten komen met bepaalde risico's. Waar mogelijk worden deze via wetgeving al zo veel mogelijk beperkt. Echter kunnen risico's nooit volledig uitgesloten worden.

Vraag 4
Bent u bereid in Europees verband te pleiten voor beveiligingseisen die uitsluiten dat verplicht voorgeschreven systemen met microfoons en camera's, zoals eCall en bestuurdersmonitoring, kunnen worden misbruikt om af te luisteren of mee te kijken?

Antwoord 4
Wij zetten ons in voor een versterking van de eisen rondom cyberbeveiliging van voertuigen om risico's te beperken. Daarnaast is onze inzet al om verplichte systemen voor te schrijven op een manier die zo min mogelijk inbreuk maakt op de privacy. Zo heeft het eCall-systeem niet standaard een actieve verbinding, maar maakt deze alleen verbinding met een netwerk wanneer deze vanuit het voertuig wordt opgestart. Voor de Advanced Driver Distraction Warning (ADDW), dat afleiding van de bestuurder tegen moet gaan, mag er bijvoorbeeld geen biometrische informatie opgeslagen worden en mogen de gegevens alleen in het voertuig verwerkt worden.

[1] AIVD *Digitale dreigingen in slimme voertuigen*, d.d. 30 september 2026, https://www.aivd.nl/actueel/nieuws/2026/09/30/digitale-dreigingen-in-slimme-voertuigen.

Daarnaast zijn, zoals aan de Kamer geïnformeerd in de Kamerbrief van 26 maart jl., de risico's van slimme voertuigen gedeeld binnen de kritieke sectoren van Infrastructuur en Waterstaat en zijn deze partijen verzocht om passende en evenredige maatregelen te nemen om hun kritieke infrastructuur te beschermen. Hierbij is afstemming gezocht met de overige leden van het kabinet, zodat ook in de andere kritieke sectoren de partijen verzocht kunnen worden om passende en evenredige maatregelen te nemen om hun kritiek infrastructuur te beschermen.

Vraag 5
Steunt u in de onderhandelingen over de herziening van de Cybersecurity Act dat de Europese Commissie de bevoegdheid krijgt om leveranciers met een hoog risico in de toeleveringsketen van verbonden voertuigen te weren? Zo nee, waarom niet?

Antwoord 5
De specifieke uitwerking per sector is nu nog niet aan de orde. De algemene lijn is dat Nederland positief staat tegenover het op EU-niveau nemen van mitigerende maatregelen om de cybersecurity binnen Europa te verbeteren, waaronder de mogelijkheid tot het nemen van maatregelen om leveranciers met een hoog risico te weren in toeleveringsketens. Wel dienen dergelijke maatregelen alleen in nauwe samenwerking met de lidstaten te worden genomen en dient er een goede risicoanalyse aan ten grondslag te liggen. Dit is de Nederlandse positie in de onderhandelingen over de herziening van de Cybersecurity Act.

Vraag 6
Op welke concrete wijze waarborgt u in de Raad en richting de Europese Commissie dat voertuigdata, zoals locatie-, camera- en microfoongegevens en gegevens van gekoppelde telefoons, niet worden opgeslagen of verwerkt bij partijen of in landen waar statelijke actoren toegang tot die gegevens kunnen afdwingen?

Antwoord 6
Zoals beschreven in het antwoord op vraag 4 zetten wij ons er voor wat betreft verplichte systemen voor in om zo min mogelijk inbreuk te maken op de privacy. Voor wat betreft de persoonsgegevens die in het algemeen in het voertuig worden verzameld geldt dat deze onder de Algemene Verordening Gegevensbescherming (AVG) vallen. Het is primair aan de fabrikanten om ervoor te zorgen dat zij aan de AVG voldoen. Dat betekent onder meer dat persoonsgegevens alleen mogen worden verwerkt in de Europese Economische Ruimte (EER), of in derde landen die een passend niveau van gegevensbescherming hebben. De Europese Commissie bepaalt welke landen dit betreft via zogeheten 'adequaatheidsbesluiten'. De Europese gegevensbeschermingsautoriteiten, in Nederland de Autoriteit Persoonsgegevens (AP), houden er toezicht op dat persoonsgegevens, waaronder die uit voertuigen, niet onrechtmatig in andere landen verwerkt worden.

Vraag 7
Geldt de regel dat defensiemedewerkers in niet-operationele voertuigen alleen ongerubriceerde informatie mogen bespreken inmiddels ook voor de rest van de rijksoverheid, inclusief bewindspersonen? Zo nee, waarom niet?

Antwoord 7
In het Besluit voorschrift informatiebeveiling 2025 (VIRBI) en in het blauwe boek (Handboek voor bewindspersonen) is opgenomen dat bijzondere (gerubriceerde) informatie uitsluitend dient te worden verwerkt (besproken) in een extra beveiligd werkgebied. Een reguliere dienstauto is dit in beginsel niet.

Het VIRBI 2025 beschrijft verder ook een aantal uitgangspunten en beveiligingsniveaus voor adequate bescherming van bijzondere informatie, die nader moeten worden ingevuld aan de hand van specifieke risicoanalyses. Hieronder vallen ook maatregelen voor het tegengaan van afluisteren.

Vraag 8
Is het rijkswagenpark, inclusief de voertuigen waarin bewindspersonen worden vervoerd, getoetst aan de adviezen uit de AIVD-publicatie over onder meer externe camera's, het koppelen van telefoons en ingebouwde navigatie? Zo nee, bent u bereid dit te laten doen?

Antwoord 8
Het bestaande rijkswagenpark is (nog) niet getoetst aan de adviezen uit de recente AIVD-publicatie. In de toekomst kunnen de adviezen van de AIVD worden meegewogen in de selectie van dienstvoertuigen.

Vraag 9
Hoe borgt u bij de opschaling van bidirectioneel laden dat er cybersecurity-eisen gelden voor laadpunten, de achterliggende beheersystemen en aggregators, zodat grote aantallen gekoppelde voertuigen niet kunnen worden ingezet om het elektriciteitsnet te verstoren?

Antwoord 9
De afgelopen jaren is er EU- en Nederlandse wetgeving geïmplementeerd waarmee de cybersecurity eisen van laadpunten, de achterliggende beheersystemen en aggregators geborgd wordt.

Laadpaalbeheerders, aanbieders van elektrische mobiliteitsdiensten en aggregators, die voldoen aan een bepaalde minimum economische omvang, vallen onder de Cyberbeveiligingswet (Cbw) die sinds augustus 2026 van kracht is in Nederland. Dit betekent dat deze partijen volgens de wetgeving beveiligingsmaatregelen moeten nemen om de cyberveiligheid te waarborgen. Ook hebben zij een meldplicht bij incidenten en vallen zij onder het toezicht van de Inspectie Leefomgeving en Transport en de Rijksinspectie Digitale Infrastructuur (RDI).

Er gelden voor fabrikanten van producten met digitale elementen, , ook cybersecurity-eisen op basis van Europese wet- en regelgeving zoals de Radio Equipment Directive 3.3 en de Cyber Resilience Act (CRA). De CRA treedt eind 2027 volledig in werking. Daarnaast heeft de laadsector een gedetailleerde set aan cybersecurity eisen ontwikkeld voor laadinfrastructuur van elektrische

voertuigen. Regionale overheden hanteren deze eisen bijvoorbeeld bij hun aanbestedingen van laadinfrastructuur.