Ministerie van Infrastructuur en Waterstaat

TER BESLISSING

Datum
7 maart 2025

Onze referentie
IENW/BSK-2025/36859

Opgesteld door
DG Mobiliteit
Dir.Wegen en Verkeersveiligheid
Voertuigen en Digitale Infrastructuur

Beslistermijn
17-03-2025

Bijlage(n)
2

Aan Minister en Staatssecretaris

nota

Beslisnota uitvoering motie Boswijk inzake nationale veiligheidsrisico's slimme (elektrische) voertuigen

Aanleiding

Het lid Boswijk (CDA) heeft op 16 april jl. een motie ingediend die de regering verzoekt om een analyse uit te voeren naar de risico's van elektrische auto's voor de nationale veiligheid en om, indien zulke risico's geconstateerd worden, opties aan te dragen om deze te mitigeren. IenW voert deze motie uit vanwege de beleidsverantwoordelijkheid van IenW over toelatingseisen en de (cyber)veiligheid van voertuigen. Middels deze nota wordt u geïnformeerd over de uitvoering van de motie en het vervolgproces en gevraagd in te stemmen met verzending van de kamerbrief naar de Tweede Kamer.

Geadviseerd besluit

- De minister wordt geadviseerd akkoord te gaan met verzending van de Kamerbrief naar de Tweede Kamer.
- De minister wordt geadviseerd in een nader vertrouwelijk overleg kennis te nemen van de staatsgeheime dreigingsanalyse (STG-C).
- Vanwege het commissiedebat auto op 20 maart wordt het opportuun geacht de Kamerbrief nog daarvoor te versturen.

Kernpunten

- Om de analyse zoals verzocht door het lid Boswijk uit te voeren, is gebruik gemaakt van de methodiek risicoanalyse nationale veiligheid van de NCTV. Op basis van deze aanpak zijn een technische werkgroep en een beleidswerkgroep opgezet.
- Het onderzoek van de technische werkgroep kijkt naar slimme (elektrische) voertuigen. Dat is breder dan de initiële motie die enkel over elektrische auto's ging. Echter gelden de mogelijke risico's die in de motie worden genoemd niet alleen voor elektrische voertuigen (EV's), maar eigenlijk voor alle 'slimme voertuigen' die verbonden zijn met het internet en ongeacht herkomst van de voertuigen.
- Aan de technische en beleidswerkgroep hebben deelgenomen: De ministeries van Infrastructuur en Waterstaat, Economische Zaken, Buitenlandse Zaken, Financiën en Defensie, alsmede voertuigenautoriteit RDW, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationaal Cyber Security Centrum (NCSC) en de Autoriteit Persoonsgegevens (AP). Ook is het Ministerie van Klimaat en Groene Groei geconsulteerd.

- Uit het onderzoek van de technische werkgroep zijn een aantal scenario's naar voren gekomen die een mogelijk risico vormen voor de nationale veiligheid van Nederland. De beschrijving van de scenario's alsmede de risicobeoordeling op die scenario's geven inzicht in nationale veiligheidsrisico's en zijn daarom niet geschikt voor openbaarmaking.
- De risicoanalyse van de technische werkgroep is vanwege de gevoeligheid departementaal vertrouwelijk (DEP-V) en zal niet openbaar met de Kamer gedeeld worden. De Kamer wordt aangeboden om in een vertrouwelijke technische briefing over de dreigingsanalyse (STG-C) en risicoanalyse geïnformeerd te worden.
- Auto's zijn een vorm van geavanceerde consumentenelektronica met een wereldwijde leveranciersketen. Dat maakt het nemen van maatregelen complex. De vertrouwelijke risicoanalyse verkent mogelijke maatregelen. Voor verstrekkende maatregelen is veelal aanvullend onderzoek vereist.
- Wel valt uit de onderzoeksresultaten al op te maken dat op dit moment het inzicht in wat voertuigen allemaal aan persoonsgegevens verwerken, waarom ze dit doen, waar deze persoonsgegevens blijven en wat er verder mee wordt gedaan, beperkt is. Dit wordt nader onderzocht door IenW, AP, ACM, RDI en RDW.

Krachtenveld
- De beantwoording is binnen IenW afgestemd met de directies DGMo/WV, DGMo/DUMO en DGMI/Internationaal.
- De beantwoording is interdepartementaal afgestemd met de leden van de beleidswerkgroep.
- Defensie heeft meegeschreven aan het kopje "defensieterreinen" in de Kamerbrief.

Informatie die niet openbaargemaakt kan worden

Veiligheid van de staat

[redacted]

Veiligheid van de staat

[redacted]

Datum
7 maart 2025

Onze referentie
IENW/BSK-2025/36859

Opgesteld door
DG Mobiliteit
Dir.Wegen en Verkeersveiligheid
Voertuigen en Digitale Infrastructuur

Aan
Minister en Staatssecretaris

Bijlage(n)
2

- Veiligheid van de staat

Datum
7 maart 2025

Onze referentie
IENW/BSK-2025/36859

Opgesteld door
DG Mobiliteit
Dir.Wegen en Verkeersveiligheid
Voertuigen en Digitale Infrastructuur

Aan
Minister en Staatssecretaris

Bijlage(n)
2

Toelichting

Internationale / Europese context
De internationale veiligheidssituatie is de afgelopen jaren sterk verslechterd en dit raakt Nederland. Statelijke en niet-statelijke actoren bedreigen in toenemende mate de nationale veiligheidsbelangen van het Koninkrijk. We zien nu al dat Nederland doelwit is van hybride aanvallen, zoals cyberoperaties, spionage en sabotage. Geopolitieke ontwikkelingen en in het bijzonder de Russische agressieoorlog in Oekraïne hebben hierop een versterkend effect.

Verenigde Staten
Op 16 januari jl. heeft de VS een verbod gepubliceerd op het gebruik van Russische en Chinese hard- en software in alle in de VS verkochte voertuigen. Het verbod ziet met name op 'vehicle connectivity systems' en 'automated driving systems'. Volgens de regel mogen nieuwe auto's vanaf 2026 ("model year") geen software hebben van Chinese/Russische afkomst, en vanaf 2029 ("model year") geen hardware meer. Nederland maakt overigens een eigenstandige afweging met inzet van onze eigen nationale veiligheidsanalyses, -maatregelen en bijbehorend instrumentarium. Voor het maken van een goede analyse heeft Nederland vanzelfsprekend contact met andere landen.

China
China heeft zelf al intern maatregelen genomen om het gebruik van bepaalde voertuigen strenger te reguleren. Zo zijn Tesla's verboden in de buurt van o.a. overheidsgebouwen of vliegvelden. Dit is mede aanleiding geweest voor het indienen van de motie.

EU
De Europese commissie is inmiddels eigenstandig onderzoek gestart naar de mogelijke cybersecurity risico's van 'connected automated vehicles'. Bij dit onderzoek worden zowel technische als niet technische factoren meegenomen. Nederland is betrokken bij de risicobeoordeling en zal daarbij putten uit de onderzoeksresultaten van de TW. Naar verwachting presenteert de commissie in april de resultaten.

Politieke context
Op 8 augustus jl. heeft het lid Boswijk Kamervragen gesteld aan de ministers van BHO en BZ over de stand van zaken van de uitvoering van zijn motie. In reactie daarop is de Kamer destijds geïnformeerd over de voorgenomen afronding van het onderzoek voor het einde van 2024. In de Kamerbrief over de stand van zaken voertuigautomatisering van 10 december jl. is aangekondigd dat de Kamer voor het einde van Q1 2025 geïnformeerd zou worden.

Tevens heeft lid Boswijk bij de begrotingsbehandeling van BZ op 21 november jl. een tweede motie ingediend, waarin hij verzoekt de economische risico's van alle mobiliteitsproducten uit China mee te nemen in het onderzoek van de TW. De uitgevoerde risicoanalyse kijkt reeds naar de technische aspecten van voertuigen ongeacht herkomst en is daarmee al breder dan de initiële scope. In het

aangekondigde verdiepende onderzoek zullen de technische risico's van bussen en vrachtwagens nog onderzocht worden.

Bijlagen

Volgnummer	Naam	Informatie
1	Kamerbrief beantwoording motie Boswijk – nationale veiligheidsrisico's slimme (elektrische) voertuigen	Kamerbrief ter publicatie
2	Risicoanalyse technische werkgroep motie Boswijk	Niet voor openbaarmaking

Datum
7 maart 2025

Onze referentie
IENW/BSK-2025/36859

Opgesteld door
DG Mobiliteit
Dir.Wegen en Verkeersveiligheid
Voertuigen en Digitale Infrastructuur

Aan
Minister en Staatssecretaris

Bijlage(n)
2