Ministerie van Infrastructuur en Waterstaat

> Retouradres Postbus 20901 2500 EX Den Haag

De voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

DG Mobiliteit
Dir.Openbaar Vervoer en Spoor

Postbus 20901
2500 EX Den Haag

Uw kenmerk
2026Z03781

Onze referentie
IENW/BSK-2026/71821

Bijlage(n)
1

Datum 26 mei 2026
Betreft Beantwoording Kamervragen van het lid Van den Berg (JA21) over mogelijke "kill switch" opties in Chinese OV-bussen (ingezonden 26 februari 2026)

Geachte voorzitter,

Hierbij bied ik u de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid Van den Berg over het bericht ‘Chinese ‘kill switch’ in bussen zorgt voor onrust in Brabant: ‘Serieus veiligheidsvraagstuk’. De vragen werden ingezonden op 26 februari 2026, met kenmerk 02026Z03781.

Hoogachtend,

Mede namens de Staatssecretaris van Digitale Economie en Soevereiniteit,

DE STAATSSECRETARIS VAN INFRASTRUCTUUR EN WATERSTAAT,

Annet Bertram

DG Mobiliteit
Dir.Openbaar Vervoer en Spoor

Onze referentie
IENW/BSK-2026/71821

1. **Heeft u kennisgenomen van de berichtgeving over mogelijke “kill switch”/remote control-functionaliteiten in elektrische bussen die in Nederlandse concessies worden ingezet? [1]**

   Ja, daar heb ik kennis van genomen.

2. **Deelt u de analyse dat openbaar vervoer in de praktijk vitale infrastructuur is en dat digitale afhankelijkheden in rollend materieel daarom een nationaal veiligheids- en continuïteitsvraagstuk kunnen vormen? Zo nee, waarom niet?**

   Dit beeld is op dit moment nog niet volledig. Binnen de cyclus vitaal, die onderdeel is van de Aanpak vitaal, zijn zowel (delen van) het vervoer over het (hoofd)wegennet, als het vervoer van personen en goederen over (hoofd)spoorweginfrastructuur aangemerkt als vitaal proces. Binnen deze vitale processen zijn vervolgens specifieke vitale aanbieders aangewezen. Het openbaar vervoer als geheel is binnen deze systematiek niet als vitaal proces aangewezen. De nieuwe Wet weerbaarheid kritieke entiteiten bevat wel de sector openabaar vervoer. Daarom zal er op basis van de Wwke voor de sector openbaar vervoer een sectorale risicobeoordeling worden uitgevoerd. Hierin worden alle relevante natuurlijke en door de mens veroorzaakte risico’s meegenomen. Op basis van de uitkomsten van deze risicobeoordeling kan dan een besluit worden genomen of OV vitale infrastructuur is en welke subprocessen binnen openbaar vervoer en welke aanbieders eventueel als kritiek worden aangewezen.

   De verantwoordelijkheid voor digitale afhankelijkheden ligt in dit geval primair bij de onderneming zelf. Toch wordt er bij de beoordeling van risico’s voor de aangewezen vitale aanbieders, binnen en buiten de spoorsector, alsnog zowel naar de fysieke, economische als digitale risico’s gekeken. Deze aanpak wordt verder versterkt met de implementatie van de aanstaande Cyberbeveiligingswet (Cbw) en de Wet Weerbaarheid Kritieke Entiteiten (Wwke).

   Tevens is de inzet van het kabinet er in algemene zin op gericht om de Europese capaciteit te vergroten, eenzijdige afhankelijkheden van derde landen af te bouwen en zoveel mogelijk te diversifiëren, ook op digitaal vlak.

3. Kunt u bevestigen dat moderne (elektrische) bussen doorgaans beschikken over functionaliteiten voor remote diagnostics en (over-the-air) software-updates, en dat dergelijke functies ook risico's voor continuïteit en sabotage of ongewenste beïnvloeding kunnen meebrengen?

Moderne bussen, waaronder elektrische bussen, zijn in toenemende mate uitgerust met functionaliteiten voor het op afstand uitlezen van voertuigen (*remote diagnostics*) en het op afstand (*over-the-air*) doorvoeren van software-updates. Deze functies kunnen efficiënter onderhoud mogelijk maken en stellen fabrikanten in staat om noodzakelijke software- en beveiligingsupdates tijdig uit te rollen. Dergelijke digitale functionaliteiten brengen echter ook mogelijke risico's met zich mee, onder meer op het gebied van spionage en sabotage. Zoals aangekondigd in een kamerbrief van dit jaar[1] zijn deze risico's van slimme voertuigen nader onderzocht.

4. Kunt u een landelijk overzicht geven van welke ov-concessies in Nederland momenteel bussen inzetten van Chinese of andere niet-EU leveranciers, welke aantallen het per concessie betreft, en welke partijen het softwarebeheer uitvoeren?

In het Nederlandse openbaar vervoer worden in enkele concessies bussen ingezet van fabrikanten buiten de Europese Unie, het betreft de Chinese fabrikanten BYD en Yutong.

Van BYD rijden circa 319 bussen, voornamelijk in de concessies IJssel-Vecht en Haaglanden Streek, met daarnaast kleinere aantallen in Noord-Holland en Friesland (Waddeneilanden). Van Yutong rijden circa 250 bussen, onder meer in de concessies Zuid-Holland Noord (regio Leiden), Groningen-Drenthe en provincie Utrecht. Gezamenlijk betreft dit circa 569 bussen, ongeveer 21% van het totale aantal zero-emissiebussen in het Nederlandse openbaar vervoer. Dit is de stand per 1 januari jl.[2]

Het beheer en onderhoud van voertuigsoftware is de verantwoordelijkheid van de concessiehouder en wordt in de praktijk veelal uitgevoerd door leveranciers en onderhoudspartijen.

5. Is bij het Rijk bekend of in meer Nederlandse concessies bussen rijden of besteld zijn waarbij de fabrikant of een gelieerde partij technisch in staat is om op afstand rijfuncties te beperken, voertuigen stil te zetten, of kritieke subsystemen (zoals

[1] Kamerstuk 30281, nr. 331

[2] Monitor vierde kwartaal 2025: 330 zero-emissiebussen afgeleverd | Zero Emissie Bus

aandrijving of batterijmanagement) te beïnvloeden? Zo ja, om welke concessies gaat het? En welke risico's spelen daar?

Nee, dit is niet bekend.

6. Klopt het dat decentrale concessieverleners niet altijd kunnen uitsluiten dat voertuigen op afstand kunnen worden beperkt of uitgeschakeld? Vindt u het acceptabel dat hierover geen eenduidige landelijke norm bestaat?

Ja, dat klopt. Binnen een OV-concessie ligt de operationele verantwoordelijkheid voor het ingezette materieel bij de concessiehouder en dus niet bij de concessieverlener. De concessiehouder is verantwoordelijk voor het beheer, onderhoud en de inzet van het materieel. De keuze voor het materieel is gemaakt door de concessiehouder binnen de door de concessie verlenende provincie vastgestelde eisen en randvoorwaarden.

7. Deelt u de opvatting dat het onwenselijk is wanneer concessieverleners en vervoerders geen harde garanties kunnen geven over het uitsluiten van "op afstand uitzetten door derden"? Welke verantwoordelijkheid ziet u hierin voor het Rijk?

Contractueel is vastgelegd dat het materieel moet voldoen aan Europese wet- en regelgeving en dat de concessiehouder verantwoordelijk is voor veilige en betrouwbare inzet. Er is tot nu ook geen bewijs geleverd dat ongewenste remote manipulatie daadwerkelijk mogelijk of uitgevoerd is. Navraag bij regionale concessieverleners- en houders leert dat dergelijke aantijgingen door leveranciers worden verworpen.

8. Bent u bereid om, samen met de relevante veiligheids- en cybersecuritypartners, een landelijke risicoanalyse uit te voeren naar remote access-mogelijkheden in ov-materieel en de afhankelijkheden in de digitale keten (zoals connectiviteit, cloud, onderhoud op afstand en updates)?

Op basis van de huidige inzichten en de bestaande risicobeoordelingen is er geen noodzaak om aanvullend een landelijke risicoanalyse uit te voeren naar remote access-mogelijkheden in ov-materieel en de afhankelijkheden in de digitale keten. Dit neemt niet weg dat er reeds, samen met relevante veiligheids- en cybersecurity partners, binnen de bestaande kaders en trajecten aandacht is voor digitale risico's, waaronder strategische afhankelijkheden.

9. Welke wettelijke en normatieve kaders gelden op dit moment voor cybersecurity en software-updates van bussen en andere

vormen van ov-materieel, en hoe is het toezicht en de handhaving daarop in Nederland georganiseerd?

De wettelijke kaders voor cybersecurity en software-updates voor bussen en ander (weg)voertuigmaterieel liggen vast in de Europese voertuigregelgeving rondom typegoedkeuring en de internationale normen van de Verenigde Naties Economische Commissie voor Europa (hierna: VN-ECE) die daarin zijn opgenomen. Zo vereist de verordening (EU) 2018/858 dat er gewerkt wordt in lijn met reglement nr. 155 (hierna: R155) over cybersecurity en VN-ECE Reglement nr. 156 (hierna: R156) over software-updates. Deze kaders verplichten fabrikanten om cyberrisico's te beheersen en software-updates (waaronder updates op afstand) op een beheerste en veilige wijze te organiseren via passende cybersecurity beheersystemen.

Toezicht en handhaving binnen het typegoedkeuringsstelsel vinden primair plaats via de typegoedkeuringsautoriteit die de betreffende beheersystemen typegoedkeuring heeft verleend. Dit kan de RDW zijn, maar ook een andere typegoedkeuringsautoriteit in Europa. Voor de voertuigen waarvoor de RDW de verlenende autoriteit is van R155/R156-typegoedkeuringen, past de RDW een intensief toezichtregime toe, onder meer door het verplicht stellen van een jaarlijkse audit op de beheersystemen voor cybersecurity en software-updates, waarbij ook wordt bezien hoe effectief beheersmaatregelen in de praktijk (op/aan het voertuig) functioneren.

10. Acht u deze kaders voldoende specifiek en afdwingbaar om risico's van ongewenste remote disablement of beïnvloeding in ov-concessies te minimaliseren? Zo ja, waar blijkt dat uit? Zo nee, welke aanvullingen acht u noodzakelijk?

Recent bent u geïnformeerd over het uitgevoerde onderzoek naar nationale veiligheidsrisico's van slimme (elektrische) voertuigen, waaronder ook bussen[3]. Uit dit traject is gebleken dat er cybersecurity-risico's bestaan op het gebied van sabotage en spionage. Om deze risico's te verminderen zal ik samen met relevante partnerorganisaties onder andere onderzoeken in hoeverre veranderingen in het Europese stelsel van goedkeuring de cybersecurity van voertuigen kunnen verbeteren en mij daar in Europees verband voor inzetten.

11. Welke eisen worden in de praktijk gesteld aan eigenaarschap en controle over beheeraccounts, encryptiesleutels en toegang tot voertuigsystemen, en hoe wordt geborgd dat de concessiehouder/vervoerder niet afhankelijk blijft van de leverancier voor kritieke toegang?

Voor wat betreft de eisen rondom de typegoedkeuring, zie het antwoord op vraag 9. Verder is het aan de concessiehouder om, indien gewenst, eisen te stellen aan de leverancier door middel van (contractuele) afspraken.

[3] Kamerstuk 30281, nr. 331.

12. Welke eisen worden gesteld aan logging, detectie van ongeautoriseerde toegang en incidentrespons rondom digitale verstoringen in het busmaterieel en de bijbehorende backend-systemen?

Zie het antwoord op vraag 9 en 11.

13. Welke eisen worden gesteld aan netwerksegmentatie, “least privilege” en andere basismaatregelen om te voorkomen dat (remote) onderhoudskanalen misbruikt kunnen worden?

Zie het antwoord op vraag 9 en 11.

14. Bent u bereid te komen tot landelijke minimumeisen (modelbepalingen) voor ov-concessies op het terrein van digitale soevereiniteit en cybersecurity, waaronder in ieder geval: verplichte disclosure van alle remote access-functionaliteiten; mogelijkheid tot onafhankelijk technisch onderzoek/audit vóór instroom; aantoonbare lokale operationele controle (“operator override”); en contractuele sancties bij niet-gemelde functionaliteiten?

Het Ministerie van Infrastructuur en Waterstaat is terughoudend in het meegeven van richtlijnen voor regionale concessies. Ik zal met de partijen in het Nationaal OV Beraad verkennen in hoeverre vervolgstappen wenselijk zijn.

15. Bent u bereid te onderzoeken of het mogelijk en wenselijk is om bij concessies te eisen dat onderhoud op afstand alleen kan plaatsvinden via streng gecontroleerde, tijdgebonden toegang, met beheer binnen de EU of door EU/NL-gebaseerde partijen?

Zie antwoord vraag 14.

16. Welke rol ziet de staatssecretaris Digitale Economie en Soevereiniteit in het opstellen van een rijksbreed kader voor digitale soevereiniteit bij aanbestedingen van (semi-)vitale infrastructuur zoals het openbaar vervoer, inclusief rollend materieel en bijbehorende digitale systemen?

De rolverdeling bij aanbestedingen door vitale aanbieders is als volgt. De minister van Justitie en Veiligheid is verantwoordelijk voor het vitaal stelsel, waaronder het

wetsvoorstel weerbaarheid kritieke entiteiten (Wwke, in uw Kamer behandeld op 23 maart jl.) die als doel heeft de weerbaarheid van organisaties in vitale sectoren te versterken. De minister van EZK is verantwoordelijk voor het beleid, de wetgeving en handhaving rondom aanbestedingen, waaronder de Aanbestedingswet 2012. De staatssecretaris van EZK (SEZ) is verantwoordelijk voor het dossier digitale soevereiniteit, waar onderdeel van de beleidsdiscussie is hoe we de digitale soevereiniteit beter kunnen borgen middels onder andere aanbestedingen. Bovendien is SEZ verantwoordelijk voor de vitale sector digitale infrastructuur en gezamenlijk met de staatssecretaris van BZK verantwoordelijk voor het aanbesteden van digitale diensten en technologie binnen het Rijk, inclusief diens vitale processen.

Het kabinet is zich bewust van het belang van digitale soevereiniteit bij aanbestedingen. Zo wordt in EU-verband gewerkt aan een Europees voorkeursprincipe bij aanbestedingen. Daarnaast verplicht de Wwke, na inwerkingtreding, kritieke entiteiten om hun leverancierslandschap en afhankelijkheden in kaart te brengen, zodat risicovolle (digitale) afhankelijkheden beter inzichtelijk worden.

Verder heeft het kabinet de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO 2026) vastgesteld. Uw Kamer is hierover geïnformeerd[4]. Hiermee kunnen risico's worden beperkt bij contracten met bedrijven waarbij de nationale veiligheid in het geding is. Ook wordt onderzocht of de ABRO in de toekomst van toepassing moet worden op onder meer vitale sectoren en openbaarvervoerbedrijven. Deze vraag wordt ook betrokken bij het rijksbrede programma 'Veilig Inkopen' dat o.l.v. de staatssecretaris van BZK onderzoekt welke risico's deze organisaties lopen voor de nationale veiligheid bij hun inkopen. In het 3e kwartaal van 2026 wordt de Tweede Kamer over de stand van zaken van het programma geïnformeerd.
Tot slot wordt binnen de Nederlandse Digitaliseringsstrategie bezien hoe overheidsbreed inkopen kan worden aangewend om de digitale soevereiniteit te vergroten. Ook wordt in 2025 een herziene Rijksbrede IT-sourcing strategie en handreiking vastgesteld, zodat Rijksorganisaties risico's beter kunnen beheersen bij keuzes rondom inbesteden, uitbesteden of samenwerken met de markt.

Gezien deze ontwikkelingen is de invoering van een verplichtend Rijksbreed kader voor digitale soevereiniteit bij aanbestedingen van vitale infrastructuur momenteel niet voorzien.

17. Hoe kijkt u naar de groei van het aandeel bussen van Chinese (of andere niet-EU) leveranciers die in Nederland plaatsvindt zonder uniform nationaal toetsingskader op remote access- en ketenrisico's?

[4] Zie TK 2025/2026 26643-1438

De groei van het aandeel bussen van Chinese of andere niet-EU-leveranciers in Nederland is in beginsel een gevolg van marktwerking. De verantwoordelijkheid voor digitale afhankelijkheden ligt daarbij primair bij de onderneming zelf. Het kabinet onderkent daarbij wel het belang voor aandacht voor digitale soevereiniteit bij aanbestedingen. Zie daarnaast het antwoord op vraag 16 voor wat betreft een nationaal toetsingskader en de inzet van het Kabinet.

18. Bent u bereid om voor bestaande concessies met vervoerders en concessieverleners afspraken te maken over mitigerende maatregelen, zoals onafhankelijke technische inspectie van telematica en remote access-paden, herconfiguratie van netwerktoegang, en noodprocedures om grootschalige uitval op te vangen?

Zie antwoord vraag 14.

19. Bent u bereid richting concessieverleners te verduidelijken dat nationale veiligheid en continuïteit zwaarwegende criteria moeten zijn in de selectie- en contracteringsfase, zodat weerbaarheid niet structureel ondergeschikt raakt aan kosten- of andere beleidsdoelen?

Zie antwoord vraag 14.

20. Hoe gaat u borgen dat in toekomstige concessies de Nederlandse vervoerder/concessiehouder daadwerkelijk de volledige technische en digitale controle heeft over het ingezette busmaterieel, inclusief beheerrechten, documentatie, toegang tot diagnose- en updatefuncties en de mogelijkheid om zelfstandig te opereren bij incidenten?

Zie antwoord vraag 14.

21. Kunt u de Kamer informeren over het tijdpad waarbinnen u een landelijk overzicht van risicovolle afhankelijkheden en een set minimumeisen voor toekomstige concessies aan de Kamer zult sturen, en welke rolverdeling u daarbij voorziet tussen I&W en EZK?

Wat betreft de minimumeisen aan concessies, zie antwoord vraag 14. Wat betreft het landelijk overzicht van risicovolle strategische afhankelijkheden wil ik erop wijzen dat het kabinet vanwege de geopolitieke en diplomatieke gevoeligheid hier niet in het openbaar over communiceert. Departementen zijn verantwoordelijk voor het

uitvoeren van analyses naar risicovolle strategische afhankelijkheden in hun sectoren. Interdepartementaal coördinatie vindt plaats in de Taskforce Strategische Afhankelijkheden, onder gezamenlijk voorzitterschap van BZ en EZK. De Kamer kan in vertrouwen worden geïnformeerd over de uitkomsten van de analyses. In het verleden liep dit via de vaste Kamercommissie van EZK.

[1] Algemeen Dagblad, 21 januari 2026, 'Chinese ‘kill switch’ in bussen zorgt voor politieke onrust in Brabant: ‘Serieus veiligheidsvraagstuk" (Chinese ‘kill switch’ in bussen zorgt voor politieke onrust in Brabant: ‘Serieus veiligheidsvraagstuk’ | Tilburg | AD.nl).