2026Z03781

(ingezonden 26 februari 2026)

Vragen van het lid Van den Berg (JA21) aan de staatssecretarissen van Infrastructuur en Waterstaat en van Economische Zaken en Klimaat over mogelijke “kill switch” opties in Chinese OV-bussen

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

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?

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?

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?

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

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?

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?

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)?

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?

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?

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?

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

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

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?

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?

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?

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?

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?

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?

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?

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?

[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).