

Vergaderjaar 2024–2025

21 501-33

Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1123

**BRIEF VAN DE MINISTER VAN INFRASTRUCTUUR EN
WATERSTAAT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 april 2025

Hierbij bied ik u, mede namens de Staatssecretaris van Infrastructuur en Waterstaat – Openbaar Vervoer en Milieu, het verslag aan van de informele bijeenkomst van EU-transportministers d.d. 17–18 maart 2025. De bijeenkomst stond in het teken van het belang van militaire mobiliteit en dual-use investeringen in het kader van de Europese veiligheid en cyberveiligheid binnen de transportsector.

De Minister van Infrastructuur en Waterstaat,
B. Madlener

Verslag informele bijeenkomst van EU-transportministers d.d. 17–18 maart 2025

Tijdens de informele bijeenkomst van EU-transportministers vonden twee sessies plaats waarbij, zoals gebruikelijk, geen besluitvorming op de agenda stond. Het ging om een gedachtewisseling tussen EU lidstaten. Aan de bijeenkomst namen ook landen van de Europese Vrijhandels-associatie (EFTA) deel.

Sessie 1: militaire mobiliteit en dual-use investeringen

Het Pools voorzitterschap opende de eerste sessie met een verwijzing naar de actuele geopolitieke situatie en benadrukte daarbij het strategische belang van dual-use¹ transportnetwerken en militaire corridors. Het voorzitterschap benoemde uitdagingen zoals versterkte financiering, omdat de huidige middelen vanuit het Connecting Europe Facility (CEF) ontoereikend blijken. Daarnaast werden governance, identificatie van militaire corridors, nauwere Europese samenwerking en soepelere grensoverschrijdende militaire bewegingen genoemd als belangrijke verbeterpunten. Het voorzitterschap nodigde de EU militaire staf (EUMS)² uit ter inleiding van de bijeenkomst. In haar inleiding benadrukte de EUMS dat militaire mobiliteit de hoeksteen is voor interne veiligheid en pleitte voor praktische oplossingen zoals vereenvoudiging van regelgeving en procedures, verbetering van infrastructuur en sterkere samenwerking tussen EU en NAVO.

De Europese Commissie (hierna: Commissie) wees op de dreiging vanuit Rusland en de verminderde zekerheid van Amerikaanse steun. Ze verwees naar twee komende initiatieven: het Witboek over de toekomst van Europese defensie³ en het REARM-initiatief⁴. De Commissie riep op tot een aanzienlijke uitbreiding van de financiële middelen ten behoeve van militaire mobiliteit. Tenslotte gaf de Commissie aan later dit jaar met een lange termijn militaire strategie te komen.

De lidstaten reageerden vanuit hun eigen nationale perspectieven, maar toonden brede overeenstemming over het verruimen van financiële middelen, vermindering van administratieve lasten en het strategisch integreren van dual-use infrastructuur binnen Europese veiligheidsplannen. Een aantal landen vroeg om uitbreiding en flexibilisering van de financiering, met name buiten de bestaande TEN-T-corridors. Verschillende lidstaten benadrukten vooral de noodzaak tot vermindering van bureaucratie, vereenvoudiging van vergunningprocedures en standaardisering voor grensoverschrijdend militair transport. Een aantal lidstaten legde verband tussen militaire mobiliteit en bredere strategische veiligheid en bepleitte nauwere integratie met NAVO-standaarden en plannen. Daarnaast vroegen verschillende lidstaten, waaronder Nederland, aandacht voor onderhoud, modernisering en betere benutting van bestaande infrastructuur, terwijl andere landen benadrukten dat

¹ *Dual-use* refereert hierbij naar infrastructurele projecten die zowel civiele als militaire mobiliteit verbeteren.

² De EU Militaire Staf (EUMS) levert militaire expertise binnen de Europese Dienst voor Extern Optreden (EDED). De rol van de EUMS is het verstrekken van vroege waarschuwingen, situatiebeoordeling, strategische planning, communicatie- en informatiesystemen, conceptontwikkeling, training en opleiding, en ondersteuning van partnerschappen.

³ Het witboek is op 19 maart jl. gepubliceerd en kunt u hier lezen: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

⁴ Zie voor meer informatie: https://defence-industry-space.ec.europa.eu/document/download/13ec18d2-8366-4fc8-a4ff-2bdfdf8e1f5f_en?filename=REARM%20Europe%20factsheet%20v17_1.pdf

investerings strategisch gekozen moeten worden met oog voor economische, civiele én militaire doelen.

Nederland bracht het belang van robuuste en betrouwbare transportinfrastructuur naar voren, mede gezien de strategische rol als doorvoerland voor de NAVO. Daarbij benadrukte Nederland dat de huidige infrastructuur langs militaire corridors verouderd is en dat gerichte investeringen en cofinanciering vanuit de EU noodzakelijk zijn. Nederland pleitte ook voor een verbeterd selectieproces van dual-use projecten, voldoende capaciteit en gegarandeerde beschikbaarheid van militaire transportmiddelen in tijden van nood.

Het voorzitterschap concludeerde dat er over het algemeen overeenstemming bestaat over het belang van verhoogde financiële middelen, vermindering van administratieve lasten en betere afstemming met de NAVO ten behoeve van dual use investeringen en militaire mobiliteit. Ten slotte werd geconcludeerd dat snelheid, flexibiliteit en praktische invulling van dual-use infrastructuur geen theoretisch vraagstuk meer zijn, maar een dringende en concrete noodzaak.

Sessie 2: Cybersecurity in de Transportsector

Het Pools voorzitterschap benadrukte in de tweede sessie over cybersecurity in de transportsector het groeiende belang van cybersecurity door de toenemende afhankelijkheid van digitale systemen. Het voorzitterschap onderstreepte dat vooral digitale infrastructuur en publieke sectoren vaak doelwit zijn van cyberaanvallen.

De Commissie wees erop dat cyberaanvallen zowel in aantal als complexiteit sterk toenemen, mede door het gebruik van kunstmatige intelligentie. Zij benadrukte het belang van een volledige en effectieve toepassing van bestaande regelgeving, zoals de NIS2-richtlijn, de Cyber Resilience Act (CRA) en de Cyber Solidarity Act (CSA). De Commissie waarschuwde tegen overmatige extra regelgeving om administratieve lasten beperkt te houden. Specifieke aandacht werd gevraagd voor kwetsbare sectoren zoals lucht- en maritiem vervoer, waarvoor strikte normen noodzakelijk zijn, evenals voor het versterken van het *European Rail Traffic Management System* (ERTMS)⁵. De Commissie stelde ook duidelijk dat cybersecurity een gedeelde verantwoordelijkheid is tussen de publieke en private sectoren en vroeg daarom om meer samenwerking, training en regelmatige analyses van kwetsbaarheden.

Op uitnodiging van het voorzitterschap gaf het EU-Agentschap voor cyberbeveiliging (ENISA)⁶ een inleiding. Ze benadrukte dat de transportsector momenteel de op één na meest aangevallen sector binnen Europa is, vooral vanwege toenemende digitalisering. ENISA pleitte voor frequente penetratietesten, betere samenwerking met leveranciers en financiële ondersteuning voor bedrijven met beperkte eigen middelen. Tot slot wees ENISA op het belang van eenvoudige maatregelen, zoals het snel toepassen van updates, die veel cyberincidenten kunnen voorkomen.

Ook de lidstaten onderstreepten eensgezind de noodzaak van nauwe Europese uitwisseling en het belang van cyberveiligheid. Zo pleitten verschillende landen nadrukkelijk voor strategische samenwerking, gedeelde investeringen en het uitwisselen van best practices en infor-

⁵ ERTMS staat voor European Rail Traffic Management System en is de standaard voor treinbeveiliging in Europa. Zie ook: <https://www.ertms.nl/home/default.aspx>

⁶ ENISA bevordert en versterkt de cyberveiligheid in de EU door beleidsondersteuning, certificering, samenwerking en bewustwording. Zie ook: <https://www.enisa.europa.eu/>

matie. Daarnaast wezen landen op specifieke kwetsbaarheden binnen bepaalde transportsectoren, waaronder spoorvervoer, luchtvaart en satellietssystemen. Zij vroegen extra aandacht en financiële steun, zoals bijvoorbeeld vanuit het Next Generation EU-fonds. Een aantal landen vestigde vooral aandacht op praktische maatregelen, capaciteitsopbouw en het aanpakken van structurele tekorten aan cybersecurity-experts via trainingen en samenwerking met de private sector. Ten slotte benadrukten enkele landen dat verdere regelgeving minder wenselijk is en dat de nadruk moet liggen op een betere uitvoering en handhaving van bestaande richtlijnen zoals de NIS2, CRA en CSA.

In haar interventie benadrukte Nederland haar inzet voor versterkte cybersecurity binnen de transportsector, met name door implementatie van de NIS2-richtlijn en afstemming met sectorale EU-regelgeving. Nederland noemde als grote uitdagingen vooral de brede toepassing van *Industrial Automation and Control Systems* (IACS). Daarbij is de afhankelijkheid van satellietnavigatiesystemen een kwetsbaarheid. Om hierbij de risico's te verminderen, zet Nederland in op het versleutelde Galileo PRS-signaal en onderzoekt zij de mogelijkheden om het Europese Galileo als standaard te gebruiken voor het transport.

Het voorzitterschap sloot de sessie af door te benadrukken dat cybersecurity essentieel is voor alle vervoersmodaliteiten. Tijdens de sessie werd volgens het voorzitterschap het belang onderstreept van een snelle implementatie van bestaande Europese regelgeving en werd vooral aangedrongen op verbeterde en snellere informatiedeling over cyberdreigingen en aanvallen. Digitalisering en cyberveiligheid raken iedere lidstaat in meerdere of mindere mate. Bewustwording, praktische samenwerking en snelle uitwisseling van informatie tussen lidstaten zijn daarom noodzakelijk.