

Vergaderjaar 2024–2025

21 501-33

Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1115

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

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 maart 2025

Hierbij ontvangt u de geannoteerde agenda van de informele bijeenkomst van EU-transportministers d.d. 17–18 maart a.s. te Warschau, Polen.

Er is nog geen formele agenda voor de informele bijeenkomst gepubliceerd. De inhoud van deze geannoteerde agenda geeft daarom de meest recente stand van zaken weer, gebaseerd op de eerste informatie die van het Poolse voorzitterschap is ontvangen. Mocht de formele agenda op belangrijke punten veranderen, dan wordt u hierover geïnformeerd in de beantwoording van het schriftelijk overleg dat gepland staat op 6 maart a.s.

De Minister van Infrastructuur en Waterstaat,
B. Madlener

De Staatssecretaris van Infrastructuur en Waterstaat,
Ch.A. Jansen

I. Geannoteerde agenda

Het Pools voorzitterschap organiseert op 17–18 maart a.s. de informele bijeenkomst van EU-transportministers in Warschau, Polen. Tijdens de informele bijeenkomsten vindt er geen besluitvorming plaats. In eerdere communicatie heeft het Pools voorzitterschap aangegeven dat de bijeenkomst zich vooral zal richten op de weerbaarheid van transport. Hierbij zal naar verwachting een sessie plaatsvinden over civiel-militaire transportinfrastructuur en een sessie over weerbaarheid van transportinfrastructuur en cyberveiligheid.

Deze geannoteerde agenda geeft in brede zin een schets van de verwachte onderwerpen en de inzet hierop van het kabinet.

Civiel-militaire transportinfrastructuur

De internationale veiligheidssituatie is de afgelopen jaren verslechterd. Dit heeft ook gevolgen voor de Nederlandse transportinfrastructuur, die nu geconfronteerd wordt met een toename van hybride dreigingen, met onder meer het risico op sabotage. In het kader daarvan is er binnen de EU een toenemende aandacht voor civiel-militaire transportinfrastructuur. Het Pools voorzitterschap zal daarom naar verwachting tijdens de informele bijeenkomst een sessie organiseren over dit thema. Van belang hierbij is het EU-actieplan militaire mobiliteit 2.0 (2022–2026)¹ dat streeft naar snelle en efficiënte verplaatsing van strijdkrachten.

In antwoord op vragen van de leden Olger van Dijk en Six-Dijkstra² is aangegeven dat er voor het treffen van infrastructurele maatregelen voor zwaar militair transport op dit moment geen specifieke (aparte) financiële middelen beschikbaar zijn bij de Ministeries van Defensie en IenW. De Commissie beschikt over financieringsprogramma's voor co-financiering van infrastructurele projecten die zowel civiele als militaire mobiliteit verbeteren (*dual-use*). Het belangrijkste instrumentarium van de Commissie dat ingezet kan worden voor *dual-use* TEN-T projecten is het financieringsprogramma *Connecting Europe Facility* (CEF). *Dual-use* projecten zijn infrastructuurprojecten die bijdragen aan de doelstellingen van het civiele en militaire TEN-T netwerk.

In het lopende Meerjarig Financieel Kader (MFK) (2021–2027) is er binnen CEF Transport € 1,69 miljard gereserveerd voor TEN-T militaire mobiliteit. Dit budget is inmiddels al helemaal uitgeput. De hoogte van het toekomstige budget in het CEF voor militaire mobiliteit wordt bepaald tijdens de onderhandelingen voor het nieuwe MFK (ingaaand in 2028). Naar verwachting zal de Commissie halverwege 2025 een voorstel presenteren voor dit nieuwe MFK. Het Pools voorzitterschap zal naar verwachting het belang van cofinanciering van *dual-use* infrastructuur onder de aandacht brengen.

De Europese Rekenkamer heeft op 5 februari jl. een speciaal verslag over militaire mobiliteit gepubliceerd waarin geconcludeerd wordt dat het EU-actieplan een solide basis biedt, maar dat de impact versterkt kan worden. De Rekenkamer heeft verschillende aanbevelingen gedaan om de voorspelbaarheid van financiering en de selectie van *dual-use* projecten te verbeteren, waaronder door te onderzoeken of het mogelijk is het overige (reguliere) CEF-budget van het nu lopende MFK in te zetten voor projecten die ook een militair doel dienen. In eerste instantie wordt dit door het kabinet positief ontvangen, gezien de geopolitieke dreigingen.

¹ Kamerstuk 22 112, nr. 3585

² Aanhangsel Handelingen II 2024/25, nr. 438 | Overheid.nl > Officiële bekendmakingen

Europese cofinanciering van *dual-use* projecten is van groot belang voor het verbeteren van de militaire mobiliteit in de EU. Deze projecten helpen de lidstaten hun transportinfrastructuur zo aan te passen dat deze voldoet aan militaire vereisten. Het kabinet hecht hier bijzonder veel belang aan, mede als trekker voor het PESCO-project militaire mobiliteit.³

Het is relevant om te vermelden dat Nederland een belangrijk doorvoerland voor de NAVO is. Er zijn al meerdere militaire transporten via weg en spoor gefaciliteerd middels het *Host Nation Support*.⁴ Deze transporten zullen naar verwachting in aantal en omvang toenemen. Om een soepel verloop te waarborgen, onderzoeken de Ministeries van IenW en Defensie samen met ProRail en Rijkswaterstaat hoe een soepel verloop van militaire transporten in verschillende crisis- en conflictsenario's kan worden gegarandeerd. Daarnaast zijn aanpassingen in (internationale) wet- en regelgeving nodig, waarbij het kabinet inzet op Europese samenwerking. Specifiek voor de havens vinden er diverse gesprekken plaats tussen havenbedrijven en de Ministeries van Defensie en IenW inzake de militaire mobiliteit.

Weerbaarheid transportinfrastructuur en cyberveiligheid

Cybersecurity is één van de onderwerpen onder weerbaarheid. De weerbaarheidsopgave dekt zowel cyber als security. Een adequate aanpak van cybersecurity van transport is vanwege de huidige geopolitieke situatie van toenemend belang voor Nederland. Nederland zet in op verbetering van de cybersecurity via de implementatie van de Network and Information Security (NIS2) richtlijn in nationale wetgeving: de Cyberbeveiligingswet (CBW).⁵ Via de implementatie van deze richtlijn en via deze wet wordt de transportsector (alle modaliteiten: lucht, spoor, water en weg) weerbaarder gemaakt tegen cyberdreigingen en cyberaanvallen.⁶

De NIS2-richtlijn volgt de NIS1-richtlijn op (sinds 2016 van kracht en geïmplementeerd in de Wet beveiliging netwerk en informatiesystemen). De Commissie introduceerde NIS2 ten behoeve van betere minimumharmonisatie, een gelijk spelveld en een verbeterd cybersecurityniveau in de EU. Alle EU lidstaten moeten de NIS2-richtlijn implementeren. De implementatie van de NIS2-richtlijn is echter complex gebleken. Bijna alle lidstaten, inclusief Nederland, hebben de implementatiedeadline van 17 oktober 2024 niet gehaald.

Ook onder de Nederlandse Cybersecuritystrategie (NLCS) wordt gewerkt aan het versterken van de digitale weerbaarheid van de transportsectoren. Via meerdere cyberweerbaarheidsprogramma's wordt samen met de organisaties in de sectoren gewerkt aan het vergroten van de cyberweerbaarheid. Een nadere toelichting per modaliteit is hieronder opgenomen.

Wegen

Voor wegen werken we aan een meerjarenprogramma instandhouding. Een groot aantal knelpunten voor maatschappelijke weerbaarheid en militaire dreiging wordt in het meerjarenprogramma aangepakt

³ PESCO (Permanent Structured Cooperation) is een defensiesamenwerkingsverband binnen de Europese Unie. Het werd in 2017 opgericht en stelt deelnemende EU-lidstaten in staat om nauwer samen te werken op het gebied van defensie en veiligheid. Zie: <https://www.pesco.europa.eu/>

⁴ De zogeheten Host Nation Support houdt in dat de verplaatsing van NAVO-militair personeel en materieel ondersteuning krijgt van het land waar de verplaatsing plaatsvindt.

⁵ Kamerstuk 22 112, nr. 3868

⁶ Ook van belang is de implementatie van de Richtlijn Veerkrachtige Entiteiten (CER) in nationale wetgeving: de Wet weerbare kritieke entiteiten.

Spoor

Ook de spoorsector moet zich wapenen tegen militaire en hybride dreigingen. De weerbaarheidsopgave gaat over beschermen, beveiligen en herstellen van vitale infrastructuur, en omvat governance, logistiek (opslag, elektriciteit, etc.) en cybersecurity. Het programma ter verhoging van de weerbaarheid van de spoorsector⁷ wordt daarom verder geïntensiveerd.

Er is een kans dat Nederland, als NAVO-lidstaat, betrokken raakt bij een gewapend conflict. Daarom heeft het kabinet hoge prioriteit gegeven aan de Rijksbrede Weerbaarheidsopgave. IenW werkt hier reeds aan voor de spoorsector via het actieprogramma Spoor. Op basis van de geopolitieke ontwikkelingen bekijkt IenW gezamenlijk met de spoorsectorpartijen (m.n. ProRail) hoe dit programma verder geïntensiveerd kan worden en met welke nieuwe ontwikkelingen rekening gehouden moet worden.

Luchtvaart

Naast de NIS2 gelden voor de luchtvaartsector specifiek nog andere eisen die zien op het informatiebeveiligingsbeleid bij luchtvaartorganisaties en bevoegde luchtvaartautoriteiten, waaronder Part-IS (Information Security) en AVSEC (Aviation Security). Part-IS richt zich op het beschermen van gevoelige informatie tegen cyberdreigingen, ongeautoriseerde toegang en datalekken. AVSEC heeft betrekking op beveiliging van de burgerluchtvaart tegen opzettelijke dreigingen zoals terrorisme en sabotage. In EU verband (EASA⁸, Commissie en lidstaten) wordt er gekeken naar de overlap tussen de NIS2 richtlijn en de verschillende luchtvaartregimes die zien op informatiebeveiligingsbeleid.

Maritiem

Voor de nautische en logistieke processen in de Nederlandse zeehavens vormen digitale aanvallen een steeds groter risico. De Branche Organisatie Zeehavens (BOZ), het Ministerie van IenW en de NCTV hebben daarom een aanpak ontwikkeld en vastgelegd in de Cyber Strategie Nederlandse Zeehavens.⁹ Daarnaast is er een landelijk cybersecurity-platform genaamd «FERM» gelanceerd, dat in november jl. een Havenbreed Incident Responspan¹⁰ heeft gepresenteerd.

⁷ Kamerstuk 29 893, nr. 270

⁸ Europees Agentschap voor veiligheid van de luchtvaart

⁹ Nederlandse zeehavens en FERM lanceren landelijk cybersecurity platform | Port of Rotterdam

¹⁰ Zie: Havenbreed-IRP-versie-november-2024.pdf