

## Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

### 1860

Vragen van de leden **Paternotte** en **Podt** (beiden D66) aan de Ministers van Buitenlandse Zaken en van Infrastructuur en Waterstaat over *de uitspraken van Commandant der Strijdkrachten van Estland over Russische activiteiten in de Baltische regio met betrekking tot GPS-verstoringen* (ingezonden 5 februari 2024).

Antwoord van Minister **Bruins Slot** (Buitenlandse Zaken), mede namens de Ministers van Infrastructuur en Waterstaat en van Defensie (ontvangen 29 mei 2024).

#### Vraag 1

Hoe interpreteert u de recente stelling van de commandant van de Estse strijdkrachten over de toename van GPS-storingen in Oost-Europa, die mogelijk verband houden met Russische verstoringactiviteiten?

#### Antwoord 1

Het kabinet is bekend met deze stelling. Er zijn vier wereldwijde *Global Navigation Satellite System* (GNSS) satellietnavigatiesystemen waarvan de bekendste twee het Europese Galileo en het Amerikaanse GPS zijn. Het kabinet is van mening dat het verstoren van satellietnavigatie tot ernstige ontregeling kan leiden met de daarbij behorende veiligheidsrisico's, onder andere van de commerciële lucht- en scheepvaart. De waargenomen toename in dergelijke storingen kan gezien worden als een destabiliserende hybride dreiging van Rusland en wordt gezien als zorgelijk.

#### Vraag 2

Welke maatregelen overweegt het kabinet, gezien de zorgen over GPS-storing die luchtvaartmaatschappijen, smartphones en wapensystemen treft, om de luchtvaartsector en andere kritieke infrastructuur te beschermen?

#### Antwoord 2

Nederland kent wetgeving en er zijn verschillende maatregelen van kracht om de luchtvaartsector en andere kritieke infrastructuur te beschermen tegen dergelijke verstoringactiviteiten.

De bescherming van kritieke systemen is de verantwoordelijkheid van de sector zelf. De Wet beveiliging netwerk- en informatiesystemen (Wbni) is hier van toepassing en geldt sinds 9 november 2018. De Wbni is er op gericht om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te

voorkomen. De Inspectie Leefomgeving en Transport (ILT) houdt onder meer voor wat betreft vervoer toezicht op de uitvoering van deze wetgeving en kan waar nodig maatregelen (laten) nemen.

De Minister van Infrastructuur en Waterstaat heeft op 7 maart 2023 het rapport over de kwetsbaarheden die gepaard gaan met het uitvallen van plaats- en tijdbepaling (PNT) met GNSS, waaronder GPS en Galileo, aan de Tweede Kamer gestuurd.<sup>1</sup> In dat rapport *Inventarisatie Kwetsbaarheden Uitval Satellietdata (IKUS II)* wordt gesteld dat de afhankelijkheid van PNT met GNSS steeds verder toeneemt. Het is daarom van belang het bewustzijn van gebruikers van plaats- en tijdbepaling van mogelijke opzettelijke, niet-opzettelijke en natuurlijke verstoringen te vergroten. Daarnaast is het nodig dat die gebruikers weten wat ze tegen verstoringen kunnen doen. Daarom werkt de overheid aan een internetportaal om aan deze behoefte te voldoen. Voor de veilige navigatie van het burgerluchtverkeer hebben luchtvaartmaatschappijen samen met de vliegtuigfabrikanten procedures ontwikkeld voor verkeersvliegers hoe om te gaan met GNSS-storingen. Verkeersvliegers zijn getraind hoe te handelen met GNSS-storingen en om deze te herkennen. Binnen de internationale burgerluchtvaartorganisatie ICAO staat het onderwerp GNSS-storingen ook op de agenda en wordt gekeken op welke wijze de vliegveiligheid verder kan worden verhoogd. Tevens zijn in de wereld, waaronder in Nederland, back-up systemen op de grond aanwezig om veilige navigatie mogelijk te houden in geval van GNSS-storingen, waaronder een dekkend netwerk van verschillende typen radionavigatiebakens. Daarnaast zijn er de aanvullende systemen zoals het traagheidsnavigatiesysteem in vliegtuigen en radars van de luchtverkeersleiding.

### Vraag 3

Zijn deze verstoringen onderwerp van gesprek in de stuurgroep Vliegen over conflictgebieden? Zo nee, waarom niet?

### Antwoord 3

De rol van de stuurgroep van het convenant deling dreigingsinformatie burgerluchtvaart is het evalueren van het functioneren van de expertgroep. In de expertgroep vergaderingen wordt onder meer aandacht besteed aan GNSS-verstoringen.

### Vraag 4

Tot op welke afstand van de Russische grens beschouwt de stuurgroep vliegen over conflictgebieden het luchtruim als veilig?

### Antwoord 4

GNSS-verstoringen kunnen ver over landsgrenzen reiken. De afstand die daarbij bereikt kan worden is sterk afhankelijk van het type storingsystemen. Dit bereik kan variëren van tientallen meters tot honderden kilometers. De overheidspartijen in de expertgroep deling dreigingsinformatie burgerluchtvaart delen gevraagd en ongevraagd dreigingsinformatie met de luchtvaartmaatschappijen, zodat de luchtvaartmaatschappijen, mede gebaseerd op deze informatie, een goede risicoanalyse kunnen maken voor een veilige vluchtuitvoering buiten het Nederlandse luchtruim. Nederlandse luchtvaartmaatschappijen gebruiken de informatie in hun eigen risicoanalyses en op basis daarvan worden vliegroutes gekozen.

### Vraag 5

Kunt u commentaar geven op de potentiële risico's en implicaties van deze storingsactiviteiten op operaties van de Noord-Atlantische Verdragsorganisatie (NAVO), gezien de rol en verplichtingen van Nederland binnen het bondgenootschap?

### Antwoord 5

Satellietnavigatie wordt verstoord door enerzijds jamming (verstoring van de signalen waardoor de ontvangst van de signalen wordt bemoeilijkt of verhinderd) en anderzijds spoofing (het manipuleren en veranderen van de data zodat ontvangers van de satellietnavigatiesignalen foutieve informatie

<sup>1</sup> Tweede Kamer, vergaderjaar 2022–2023, 24 446, nr. 83.

gebruiken). Daarbij is het van belang aan te geven dat spoofing en jamming vooral van toepassing zijn op het gebruik van open (onbeveiligde) satellietnavigatiesignalen.

Ook bestaan er alternatieve PNT-systemen waarmee de risico's van storingsactiviteiten op operaties van de NAVO gemitigeerd kunnen worden. Verder is de VS bezig met het moderniseren van GPS, waarbij de algehele prestaties en capaciteiten van het systeem, zowel commercieel als militair, minder kwetsbaarheden toont voor verstoringen. Het Europese satellietnavigatiesysteem Galileo, qua techniek en prestaties het meest geavanceerde GNSS, beschikt ook over de zogenaamde Public Regulated Service (PRS). PRS betreft een hoog beveiligd satellietnavigatiesignaal dat ongevoelig is voor spoofing en betere bescherming biedt tegen jamming. Door de Minister van Infrastructuur en Waterstaat wordt, in samenwerking met onder andere het Ministerie van Defensie, gewerkt aan de invoering en het gebruik van PRS door Defensie alsook in andere vitale sectoren.

Hoewel storingsactiviteiten voor risico's kunnen zorgen voor NAVO-bondgenoten, beschikken vliegers die onder NAVO-vlag opereren en de luchtverkeersdienstverleners binnen de NAVO over de benodigde kennis en training om met dergelijke storingsactiviteiten om te kunnen gaan.

Vraag 6

Heeft Nederland, in afstemming met de NAVO en andere Europese partners, de volledige omvang van de dreiging die uitgaat van deze vermeende jamming-activiteiten in kaart gebracht, en welke stappen staan er gepland om deze risico's te beperken?

Antwoord 6

De dreiging die uitgaat van GNSS-jamming en de recente toename in dergelijke activiteiten is bij Nederland, de NAVO en andere Europese partners bekend en wordt doorlopend gemonitord.

Zoals reeds genoemd in het antwoord op vraag 5, kunnen bondgenoten gebruik maken van alternatieve PNT-systemen om de risico's van GPS-verstoringen te mitigeren. Tegelijkertijd wordt gewerkt aan de invoering en het gebruik van Galileo PRS in Nederland.

Vraag 7

Bestaat er, in het licht van deze ontwikkelingen, een strategie of discussie binnen het Nederlandse kabinet of met NAVO-bondgenoten over het vergroten van de collectieve cyberdefensiecapaciteiten om potentiële bedreigingen van elektronische oorlogsvoering tegen te gaan? Zo nee, waarom niet?

Antwoord 7

GNSS verstoringen worden in zowel nationaal als NAVO-verband besproken. In NAVO-verband is er voor Elektromagnetische Operaties (EMO) beleid ontwikkeld. Ook is er binnen de NAVO een strategie overeengekomen over het gebruik van het elektromagnetisch spectrum (EMS). Deze strategie is zowel gericht op de verdere ontwikkeling van eigen militaire elektromagnetische capaciteiten als op de verdediging tegen vijandige EMS-wapensystemen tijdens gevechtshandelingen.

Daarnaast heeft de NAVO een PNT & Navigation Warfare Policy (2022), dat maatregelen voorschrijft die de gevolgen van GNSS-verstoringen mitigeren.

Vraag 8

Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord 8

Ja.