Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 592 Defensienota 2024 – Sterk, slim en samen

Nr. 44

BRIEF VAN DE STAATSSECRETARIS VAN DEFENSIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 september 2025

De gevechtskracht van Defensie bestaat meer en meer uit IT. Het Netherlands Armed Forces Integrated Network (NAFIN) speelt een belangrijke rol bij het waarborgen van militaire operaties, nationale veiligheid en bondgenootschappelijke communicatie. Het NAFIN heeft een belangrijke rol in de Nederlandse samenleving, welke duidelijk werd door een technische storing in augustus 2024. De Minister van Defensie heeft uw Kamer geïnformeerd over deze storing[1].

Zoals genoemd in de reactie op het rapport «De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN» van de Algemene Rekenkamer[2] en in de reactie op de «Evaluatie NAFIN storing[3]» heeft Defensie onderzoek gedaan of het NAFIN aangemerkt moet worden als vitale infrastructuur. In het onderzoek is de motie van de leden Heite en Kathmann[4] van de Tweede Kamer meegenomen. Hierin wordt Defensie verzocht te rapporteren aan de Tweede Kamer over de veiligheid van het NAFIN. Daarnaast wordt Defensie verzocht om te onderzoeken hoe voldaan kan worden aan de randvoorwaarde dat Defensie in elke situatie zelf de regie moet hebben over het NAFIN, terwijl het voldoet aan de veiligheidseisen van een vitaal netwerk. De Staatssecretaris van Defensie heeft u geïnformeerd dat met het aannemen van de motie de scope van het onderzoek uitgebreid is, waardoor het onderzoek na het zomerreces is afgerond[5].

Achtergrond

Het NAFIN vormt de ruggengraat voor commandovoering, operatiecoördinatie en het delen van inlichtingen binnen Defensie en is essentieel voor

[1] Kamerstuk 26 643, nr. 1214 d.d. 28 augustus 2024
[2] Kamerstuk 36 592 nr. 8 d.d. 20 december 2024
[3] Kamerstuk 36 592 nr. 14 d.d. 20 maart 2025
[4] Kamerstuk 36 592 nr. 20 d.d. 11 juni 2025
[5] Kamerstuk 36 592 nr. 22 d.d. 23 juni 2025

kst-36592-44
ISSN 0921 - 7371
's-Gravenhage 2025

het functioneren van de krijgsmacht in zowel vredestijd als crisissituaties. Ook processen buiten Defensie, zoals de werking van noodnummers en de overheidsdatacenters, zijn afhankelijk van het NAFIN, waardoor het netwerk direct bijdraagt aan de autonomie van de Staat als het gaat om de nationale veiligheid. Bij de realisatie van het NAFIN, in de jaren '90, zijn door Defensie twee belangrijke eisen gesteld.

- Ten eerste mag het netwerk, gezien zijn cruciale rol voor de inzet van Defensie, nooit uitvallen: het principe van «*never out*».
- Ten tweede dient het NAFIN «*military owned and controlled*» te zijn. Dit wil zeggen dat Defensie in elke situatie zelf de regie moet hebben om het netwerk operationeel te kunnen houden.

De focus van het NAFIN lag lange tijd op kostenefficiëntie. De veranderende internationale veiligheidssituatie en de hernieuwde focus op hoofdtaak 1 vragen om een herijking van NAFIN's rol en capaciteiten. Dit vraagt om een visie op NAFIN met focus op de kerntaken, weerbaarheid en de borging van de veiligheid, zowel voor nu als in de toekomst. De Strategische Visie NAFIN is separaat met deze brief vertrouwelijk aan uw Kamer verzonden[6].

Conclusies

Het aanwijzen van het NAFIN als vitaal binnen de cyclus vitaal van de National Coördinator Terrorismebestrijding en Veiligheid (NCTV) brengt verschillende voordelen met zich mee. Zo zorgt de vitale status voor extra ondersteuning vanuit de overheid en gerelateerde instanties. Er kan beroep worden gedaan op ondersteuning van het Nationaal Cyber Security Centrum (NCSC). Belangrijk hierbij te noemen is dat Defensie beschikt over haar eigen Defensie Cyber Security Centrum (DCSC). Daarnaast ontstaat er meer inzicht in sector-overstijgende afhankelijkheden tussen vitale processen. Ook stimuleert het kennisuitwisseling en samenwerking met andere vitale sectoren, waardoor *best practices* en expertise breder kunnen worden ingezet.

Tegelijkertijd ziet Defensie enkele belangrijke nadelen aan het vitaal verklaren van het NAFIN volgens de cyclus vitaal. Zo kan volgens Defensie het coördinatieproces in crisissituaties complexer en trager worden, waardoor de snelheid en autonomie van de militaire besluitvorming onder druk kunnen komen te staan. Defensie ziet daarnaast het risico dat aansturing en escalatie in geval van crisis of sabotage niet uitsluitend bij Defensie blijven liggen, maar ingebed raken in interdepartementale procedures. Dit kan ertoe leiden dat Defensie in urgente situaties minder direct en slagvaardig kan optreden. Ten slotte vergroot de status van vitaal de zichtbaarheid van het NAFIN als essentieel onderdeel van de nationale infrastructuur. Vitale IT-infrastructuur komt hierdoor nadrukkelijker in het vizier van kwaadwillende actoren, wat het risico op doelgerichte aanvallen verhoogt.

Op basis van de Strategische Visie NAFIN heb ik besloten om het NAFIN niet onder de cyclus vitaal van de NCTV te brengen. De belangrijkste reden hiervoor is dat vitaal verklaring onder de cyclus vitaal de regie en militaire autonomie van Defensie ten aanzien van het NAFIN inperken wat in strijd is met het principe «*military owned and controlled*». Defensie wil te allen tijde de volledige regie en zeggenschap over het NAFIN behouden om zelfstandig haar kerntaken te kunnen uitvoeren. Tevens is Defensie als nationale veiligheidsorganisatie uitgezonderd van de wetten en

[6] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer

regelingen voor het aanwijzen, beschermen en reguleren van vitale infrastructuur in Nederland.

Ondanks dat ik het NAFIN niet vitaal zal verklaren binnen de overheidsdefinitie van de cyclus vitaal, beschouw ik het wel als onmisbaar voor onze nationale veiligheid. Daarom zal ik de weerbaarheid van het NAFIN versterken. Dit wordt bereikt door de veiligheidsvoorwaarden die gelden voor vitale processen en IT-infrastructuur ook van toepassing te verklaren op het NAFIN. Daarbij wordt gebruik gemaakt van bestaande wet- en regelgeving en *best practices*. Ook wordt het interne beheer, beveiliging en afspraken met leveranciers aangescherpt en alsmede de naleving van de aansluitvoorwaarden door externe gebruikers. Tot slot voert de CIO periodiek een onafhankelijke weerbaarheidsanalyse op het NAFIN uit.

Ik vertrouw erop uw Kamer hiermee voldoende te hebben geïnformeerd.

De Staatssecretaris van Defensie,
G.P. Tuinman