35728 Programma Grensverleggende IT (GrIT)

36975 Defensienota 2026 - Samen voorwaarts!

Nr. 28 Brief van de staatssecretaris van Defensie

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 september 2026

Inleiding
Met deze brief geef ik, mede naar aanleiding van het verzoek van de vaste commissie voor Defensie van 19 juni 2026[1], een overzicht van de belangrijkste IT-infrastructuurprojecten binnen Defensie. Daarbij wordt zowel ingegaan op initiatieven binnen de scope van GrIT als op relevante ontwikkelingen daarbuiten.

Dit verzoek komt tegen de achtergrond van een snel veranderende geopolitieke situatie en een razendsnel evoluerende technologische omgeving, waarin digitale transformatie essentieel is voor de paraatheid van en afschrikking door de krijgsmacht. In de Defensienota 2026 “Samen voorwaarts!”[2] en de Digitale Transformatie Strategie (DTS)[3] wordt de noodzaak onderstreept om een modern, wendbaar en interoperabel IT-landschap te realiseren, dat direct bijdraagt aan de gevechtskracht.

In de Digitale Transformatie Strategie richt Defensie zich expliciet op vijf sterk samenhangende speerpunten: (1) communicatie, (2) digitaal fundament, (3) data & AI, (4) cyber & EMS en (5) digitale wendbaarheid. Speerpunt een en twee omvatten de IT-infrastructuur waar de digitale transformatie op wordt gebouwd. Een IT-infrastructuur die modern en wendbaar is en voldoende robuust om een betrouwbare en continue werking te garanderen, is essentieel.

Afbakening
Via dit verzoek vraagt uw Kamer om inzicht in de onderlinge samenhang van de IT-infrastructuurprojecten, de bijbehorende budgetten en de strategische keuzes en randvoorwaarden. Omdat een deel van de informatie om operationele veiligheidsredenen gevoelig is, wordt in deze brief afgebakend welke gegevens openbaar gedeeld kunnen worden en welke op hoofdlijnen of geheel vertrouwelijk blijven.

Definitie
Defensie verstaat onder IT-infrastructuur het geheel van hardware, software, netwerken en diensten dat nodig is om de digitale systemen en gegevens te gebruiken en beheren. Lopende projecten die aan deze omschrijving voldoen, zijn onderdeel van het hiernavolgende overzicht. Geplande projecten blijven buiten beschouwing aangezien de scope en de financiële impact hiervan nog in ontwikkeling zijn, waardoor een betrouwbaar overzicht op dit moment niet kan worden geboden.

De selectie van IT-infrastructuurprojecten is gebaseerd op drie criteria:

1 Kenmerk 2026Z13871/2026D31132.
2 Kamerstuk 36 975, nr. 1.
3 Kamerstuk 36 592, nr. 23.

1. Strategische relevantie – een fundamentele bijdrage aan de basisarchitectuur of de operationele werking van de krijgsmacht.
2. Financiële impact – projecten met een investering van meer dan €100 miljoen of een reeds publiek gemaakte bandbreedte.
3. Afhankelijkheid – projecten die direct nodig zijn voor andere initiatieven (bijvoorbeeld een cloud-omgeving die zonder een robuuste netwerkinfrastructuur niet kan functioneren).

Deze afbakening maakt dat updates, upgrades en MidLife Updates (MLU's) buiten beschouwing blijven. In het kader van operationele veiligheid blijft wapensysteemgerelateerde IT, zoals ook geldt voor het Rijks ICT Dashboard, buiten beschouwing. Defensiebrede programma's zonder specifiek IT-infrastructuuroogmerk vallen eveneens buiten scope:

- Het programma Roger[4] valt buiten de scope, aangezien het niet voldoet aan de definitie van IT-infrastructuur.
- Het programma Defensie Open op Orde (DOO) valt buiten de scope, dit betreft een programma met IT-softwarecomponenten (toepassingen), maar geen IT-infrastructuur.

Moderne, robuuste en wendbare IT-infrastructuur is voor Defensie essentieel. Defensie heeft een aantal initiatieven geïnitieerd die gezamenlijk aan dit fundament bijdragen:

1. Programma GrIT
2. Programma FOXTROT
3. Satcom-initiatieven
4. Cloud-initiatieven

Bovengenoemde vormen de grootste, specifiek op infrastructuur gerichte initiatieven. Door continue levenscyclus- en cyberweerbaarheidsmaatregelen wordt de infrastructuur voortdurend verbeterd.

IT-infrastructuur

GrIT (Grensverleggende IT)
Het programma Grensverleggende IT (GrIT) richt zich op het toekomstbestendig maken van de IT van Defensie en is opgebouwd rond drie pijlers. Pijler 1 betreft de ontplooide operationele IT, die militairen in staat stelt om ook tijdens inzet over betrouwbare en veilige IT-voorzieningen te beschikken. Binnen Pijler 2 wordt de IT-infrastructuur gerealiseerd, waarmee de IT-dienstverlening aan Defensie wordt vernieuwd en waar bijvoorbeeld datacenters, cloudvoorzieningen en netwerken onder vallen. Pijler 3 richt zich op de IT voor eindgebruikers, zoals de moderne digitale werkplek en voorzieningen voor communicatie en samenwerking. Gezamenlijk vormen deze drie pijlers de basis voor een veilige, betrouwbare en toekomstvaste IT-omgeving die Defensie ondersteunt bij het uitvoeren van haar taken, zowel nationaal als internationaal. U wordt elk halfjaar geïnformeerd over het volledige programma via de voortgangsrapportage.

Foxtrot

[4] Het programma ROGER regelt de migratie van de huidige, verouderde SAP-omgeving naar een nieuwe, moderne softwareomgeving binnen Defensie. Hiermee wordt de digitale bedrijfsvoering vernieuwd om de ondersteunende processen efficiënter en toekomstbestendiger te maken.

Hoewel het programma Foxtrot aangemerkt is als een materieel project (conform het Defensie Materieel Proces), is het opgenomen in dit overzicht vanwege de technische samenhang met de IT-infrastructuur. FOXTROT heeft als missie het leveren van een veilige, altijd beschikbare en interoperabele IT-infrastructuur voor het “Mobiel-Uitgestegen / Te Voet” domein. Het vervangt verouderde communicatiemiddelen, implementeert zero-trust-principes voor mobiele operaties en ontwikkelt een interoperabiliteitsraamwerk voor samenwerking met nationale en internationale partners op tactisch niveau. FOXTROT koppelt aan de netwerkinfrastructuur van GrIT en maakt gebruik van cloud-faciliteiten om dynamische services aan eenheden in het veld te bieden.

Satcom (satellietcommunicatie)
Beveiligde en robuuste satellietcommunicatie is essentieel voor het wereldwijde multidomein optreden van onze krijgsmacht. In de Defensienota 2022 en 2024 is de verdere ontwikkeling van satellietcommunicatiesystemen en de versterking van bredere ruimtecapaciteiten opgenomen. Defensie maakt gebruik van een combinatie van middelen en methoden, variërend van commerciële satellieten voor laag beveiligde toepassingen, samenwerking met Europese partners voor extra beveiligde communicatie, tot aan internationale partnerschappen voor strategische satellietdiensten. Ook de ontwikkeling van een eigen satellietconstellatie past in deze ambitie, met bijbehorende essentiële IT-infrastructuur zoals data-opslag, netwerken en rekenkracht. Daarnaast wordt de relevantie van het EU-project IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) voor militaire doeleinden onderzocht.

Cloud
Zowel GrIT, Foxtrot als Satcom maken gebruik van cloud-faciliteiten. In het kader van duidelijkheid en transparantie licht ik de multicloud-strategie nader toe.

Defensie kiest voor een multicloud-aanpak, waarbij meerdere cloudplatformen van verschillende leveranciers worden ingezet. Dit omvat onder meer het eigen private cloudplatform binnen GrIT, een private cloud voor staatsgeheime informatie, public cloudomgevingen en Europese en NAVO-cloudomgevingen. Hierdoor kan per situatie de meest geschikte omgeving worden gekozen, blijft Defensie onafhankelijk van één aanbieder en kunnen data en applicaties worden verplaatst bij storingen of crises. De gezamenlijke cloud-laag levert de benodigde rekenkracht voor data-intensieve taken, wat direct bijdraagt aan de militaire slagkracht. Uniforme, eenvoudige beveiligingsregels (Zero-Trust en encryptie) borgen de veiligheid en de samenwerking met Europese en NAVO-partners.

Voor de uitvoering van de diverse initiatieven werkt Defensie intensief samen met externe marktpartijen en systeemintegrators, waarbij Defensie te allen tijde de regie behoudt. De samenwerking wordt geborgd door strikte contractuele kaders waarin eisen aan architectuur, veiligheid en kennisoverdracht zijn vastgelegd. Dit waarborgt dat Defensie niet afhankelijk wordt van één partij en dat de benodigde expertise binnen de organisatie behouden blijft. Uw Kamer is recent vertrouwelijk geïnformeerd over de staatsgeheime cloud; een cloud om staatgeheime informatie te verwerken. Dit is een van de voorbeelden van cloud initiatieven binnen Defensie. Daarnaast wordt binnen het programma GrIT het Private Cloud Platform gerealiseerd binnen Pijler 2.

Financieel overzicht
Vanwege de operationele veiligheid kan ik u geen gedetailleerd financieel overzicht per individuele component verstrekken. We informeren uw Kamer ten aanzien van het programma GrIT (vertrouwelijk) over de financiële omvang via de reguliere voortgangsrapportage en ten aanzien van het programma FOXTROT via het reguliere Defensie Materieel Proces.

Strategische samenhang
De Digitale Transformatie Strategie beschrijft de noodzaak van een eenduidige digitale keten waarin netwerken, cloud en toepassingen soepel op elkaar aansluiten. GrIT vormt het digitaal fundament waarop oude en nieuwe IT gemakkelijk aansluit. De multicloud-strategie voorziet dit fundament van de flexibiliteit die FOXTROT en andere initiatieven nodig hebben om operationeel effectief te zijn. Deze gelaagde opbouw voorkomt versnippering en maximaliseert de interoperabiliteit met Europese en NAVO-partners.

Om de samenhang tussen de fysieke infrastructuur (GrIT, Foxtrot, Cloud en Satcom) en de strategische ambities van Defensie volledig te duiden, is het relevant te vermelden dat deze fundamenten de noodzakelijke basis bieden voor de Data & AI-infrastructuur. Deze gespecialiseerde laag valt buiten de afbakening van dit overzicht, echter is deze fysieke infrastructuur essentieel om de digitale transformatie vorm te geven.

Om deze infrastructuur optimaal te benutten voor de ambities binnen het speerpunt ‘Data & AI’ van de Digitale Transformatie Strategie, is een infrastructuur nodig die verder gaat dan reguliere cloud- en netwerkdiensten. Defensie investeert daarom in de modernisering van de datacenterinfrastructuur om de benodigde rekenkracht voor data-intensieve missies te kunnen faciliteren. Centraal in deze ontwikkeling staat het Defensie Big Data Advanced Analytics Platform (DBDAAP). Dit platform fungeert als de motor voor data science binnen de organisatie en wordt doorontwikkeld binnen zowel de Laaggerubriceerde Informatievoorziening (LGI) - als de Hooggerubriceerde Informatievoorziening (HGI). Hiermee wordt gewaarborgd dat data-analyse en AI-toepassingen — afhankelijk van de classificatie en de operationele context — veilig, schaalbaar en met de benodigde rekenkracht kunnen worden uitgevoerd.

Defensie waarborgt de onafhankelijkheid van leveranciers door met open standaarden en gestandaardiseerde processen te werken. Daardoor kan eenvoudig de meest geschikte technologie worden gekozen, continu worden geïntegreerd en kan Defensie sneller inspelen op technologische innovaties zonder vast te zitten aan één partij. Een Zero-Trust-model, end-to-end-versleuteling en certificering volgens NATO- en National Institute of Standards and Technology-normen (internationaal cybersecurity raamwerk) vormen de basis voor digitale beveiliging. Tot slot wordt continuïteit gewaarborgd doordat data en toepassingen flexibel tussen verschillende cloud-omgevingen kunnen worden verplaatst bij storingen of crises.

Conclusie
Defensie geeft momenteel uitvoering aan een viertal initiatieven – GrIT, FOXTROT, Satcom en cloud – die samen de digitale basis vormen voor de modernisering van de krijgsmacht. Deze vier initiatieven zijn onderling afhankelijk en van grote strategische betekenis. Defensie investeert hiermee in een moderne, wendbare en robuuste IT-omgeving die de operationele

paraatheid, veerkracht en innovatiekracht van de Nederlandse krijgsmacht waarborgt in een voortdurend veranderende geopolitieke situatie.

Dit overzicht wordt gelijktijdig met de negende voortgangsrapportage van GrIT verzonden aan de Kamer, uiterlijk 1 oktober 2026. Deze brief benoemd de belangrijkste IT-infrastructuurprojecten. Gezien de complexiteit en gevoeligheid van dit onderwerp ben ik bereid uw Kamer, indien daaraan behoefte bestaat, hierover in een technische briefing nader te informeren. Een dergelijke briefing biedt de gelegenheid om dieper in te gaan op de onderliggende informatie en overwegingen.

De staatssecretaris van Defensie,
D.G. Boswijk