35 728 Programma Grensverleggende IT (GrIT)

Nr. 25 Brief van de staatssecretaris van Defensie

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 april 2026

Hierbij ontvangt u de achtste voortgangsrapportage van het programma Grensverleggende IT (GrIT). Deze voortgangsrapportage beslaat de periode van 1 juli 2025 tot en met 31 december 2025 en volgen de eerder gemaakte keuzes in relatie tot Hoofdtaak 1. In deze brief wil ik ingaan op het belang van moderne IT voor Defensie, de voortgang van het programma in 2025 en de verwachtingen voor 2026. U ontvangt hierbij ook de vertrouwelijke bijlage. Daarin wordt u geïnformeerd over de opbouw van het budget voor GrIT, de instandhoudingskosten van de huidige IT en verdere kostenspecificaties. Dit betreft commercieel vertrouwelijke informatie. Omdat openbaarmaking hiervan de aanbestedingsprocedure kan beïnvloeden, schade op kan leveren voor het bedrijf in kwestie en daarmee de positie van Defensie kan beïnvloeden, wordt deze bijlage vertrouwelijk aangeboden.

Met GrIT werkt Defensie aan de vernieuwing van de IT-infrastructuur van de krijgsmacht. Een moderne, veilige en robuuste digitale basis is noodzakelijk om de organisatie te ondersteunen in zowel de bedrijfsvoering als bij operationele inzet. De recente ontwikkelingen in de internationale veiligheidssituatie onderstrepen het belang van betrouwbare en toekomstbestendige IT. Militair optreden is in toenemende mate afhankelijk van informatie, digitale systemen en veilige communicatie. Met GrIT bouwt Defensie daarom aan een digitale ruggengraat die militairen in staat stelt sneller informatie te delen, beter samen te werken en weerbaar te blijven tegen digitale dreigingen.

Resultaten tweede helft 2025

De resultaten in Release 4 in de tweede helft van 2025 laten een gemengd beeld zien. In deze brief licht ik de belangrijkste resultaten hiervan uit. Er zijn positieve resultaten behaald met betrekking tot Pijler 1, waarin de ontwikkeling van de Modules Ontplooid plaatsvindt. Hieronder valt de IT-infrastructuur die wordt gebruikt bij het ontplooid operationeel optreden van de eenheden in het veld. Het gaat hierbij vooral om de oplevering van modules die samen een mobiel datacenter vormen. Hiermee hebben eenheden ook tijdens missies toegang tot IT, variërend van reguliere Defensie-e-mail tot battle management-applicaties, inclusief beveiligde verbindingen met NAVO-partners. De realisatie hiervan levert een directe bijdrage aan de ondersteuning van hoofdtaak 1 van Defensie. Zo is er vooruitgang geboekt met betrekking tot de hardware en de behuizing van de modules, die verder zijn uitgewerkt met de operationele commando’s. Ook hebben de eerste beproevingen met val- tril- en stoftesten plaatsgevonden en is de assemblage van acht varianten prototypes uitgevoerd. Bovendien is gewerkt aan het plannen, organiseren en uitvoeren van vier Proof-of-Concepts. Die helpen bij

het versneld opleveren van modules en helpen de operationele commando’s bij het leren omgaan met de nieuwe IT, zodat een goede implementatie daarvan kan worden gerealiseerd.

Op het gebied van de statische IT-infrastructuur waren er echter tegenvallers. Door vertraging in de oplevering van het Private Cloud Platform (PCP) door de leverancier is hier slechts een deel van de doelstellingen behaald, zoals ook aan uw Kamer gemeld in de beantwoording van de schriftelijke vragen (Kamerstuk 35 728, nr. 24). Het PCP is een eigen cloud platform voor Defensie, dat een veilige en flexibele cloudomgeving biedt en daarmee dus niet afhankelijk is van technologie van een van de grote *hyperscalers*. Eindgebruikers kunnen hiermee eenvoudig geautomatiseerde Private Clouddiensten aanvragen, wat bijdraagt aan de uitbreiding van de digitale capaciteit van Defensie. De oplevering van het PCP is een randvoorwaarde voor de succesvolle afronding van zowel de uitbreiding van het IT-Service Management als de migratie van applicaties in de verschillende migratiefases. Daardoor zullen ook die in latere releases worden opgeleverd.

Aanpak voor verbetering

In reactie op het niet opleveren van het PCP heeft Defensie mitigerende maatregelen genomen om de impact op het programma te beperken en alsnog voor een snelle oplevering te zorgen. In de beantwoording van de feitelijke vragen over GrIT (Kamerstuk 35 728, nr. 24) van 26 januari 2026, heb ik toegezegd daar in deze Kamerbrief op terug te komen. Van de leverancier van het PCP is nakoming en een herstelplan geëist, waarbij laatstgenoemde door externe validator PWC als positief is beoordeeld. Daarnaast heeft Defensie het PCP door de onafhankelijke organisatie Gartner laten toetsen en technisch laten valideren, waarbij Gartner concludeerde dat het ontwerp, de gekozen softwareproducten en de voorgestelde oplossing technisch solide zijn. De maatregelen van de IT-infrapartner heeft Defensie, samen met een aantal andere maatregelen, samengevoegd tot een verbeterplan dat moet leiden tot de oplevering van het PCP. Het standpunt daarbij is dat de vertraging niet tot meerkosten mag leiden.

De belangrijkste elementen zijn:

- de IT infrapartner die extra capaciteit inzet voor het leveren en integreren van de verschillende software elementen van het PCP,
- de voortbrenging wordt georganiseerd in 3-wekelijkse sprints, waardoor tussentijdse sturing beter mogelijk is,
- betere procesafspraken tussen het programma, de IT infrapartner en de beheerorganisatie op gebied van het vaststellen van technische ontwerpen, doorvoeren van veranderingen voor koppelingen van huidige IT en nieuwe IT en het testen en accepteren van opgeleverde producten,
- opgeleverde producten worden op beheerbaarheid gevalideerd door een externe partij.

Mede door bovenstaande maatregelen zijn de eerste onderdelen van het PCP conform de planning uit het herstelplan opgeleverd.

Vooruitblik programma 2026

Door de vertraging van het PCP staat release 5 in de eerste helft van 2026 in het teken van onder meer het nog openstaande werk uit voorgaande releases. Dit omvat dat het PCP gereed is voor accreditatie, het samen met de operationele commando’s realiseren van vier Proof-of-Concepts van de Modules Ontplooid en de uitbreiding van het Protected Core Network. De technische oplevering van het PCP gebeurt in release 5, waarna in latere releases de accreditatie en inbeheername hiervan volgen. Als gevolg van de vertraging van het PCP, vertragen daarmee ook de blokken service management, security en de toegang. Omdat er geen technische afhankelijkheid is van het PCP met de ontplooide IT, wordt voor pijler 1 geen vertraging verwacht. Met de realisatie van de mijlpalen in de eerste helft van 2026 wordt de beschikbaarheid van applicaties voor de gebruiker verbeterd en zijn operationele eenheden in staat beter en sneller onderling te communiceren in het veld.

De exacte consequenties van de vertraging van het PCP voor de eindmijlpaal van het programma – die nog steeds op december 2030 staat - zijn echter nog onduidelijk. In de volgende voortgangsrapportage zal ik hierop terugkomen en de mogelijke impact op de eindmijlpaal verder toelichten.

De staatssecretaris van Defensie,
D.G. Boswijk