GrIT voor digitale weerbaarheid

"Defensievisie 2035 impliceert een vernieuwing van onze Krijgsmacht"

Jeroen van der Vlugt is sinds 1 maart 2020 Chief Information Officer (CIO) van het ministerie van Defensie. Hij is verantwoordelijk voor het gecombineerde IT-portfolio van de verschillende onderdelen van de Krijgsmacht en tevens de Chief Data Officer (CDO) en Chief Security Officer (CISO). Als CIO is Van der Vlugt ook lid van de "Raad van Bestuur" van het NATO IT-agentschap (NCIA).

Na 25 jaar actief te zijn geweest in het bedrijfsleven (onder meer bij KPN, Atos, Boer & Croon en als co-founder van het consultancybureau RevelX waar hij een aantal klanten binnen de overheid adviseerde), was Jeroen van der Vlugt toe aan de stap "naar een organisatie die maatschappelijk een belangrijke rol heeft. Defensie is uniek in zijn soort. Maar er ligt ook een enorme uitdaging op het gebied van IT, data en cyber. De organisatie staat voor een belangrijke transformatie op die drie gebieden."

Voor die transformatie is een toekomstbestendige IT-infrastructuur een vereiste en daartoe heeft demissionair staatssecretaris Barbara Visser op 30 december 2020 haar handtekening gezet onder het Grensverleggende IT (GrIT) contract met het consortium Athena waarvan IBM en Atos belangrijke partners zijn. "Wij zijn heel trots dat het ons is gelukt, we hebben er als team heel veel *effort* in gestoken om dit te bereiken. We zijn bijna vijf jaar bezig geweest om naar dit punt toe te werken en we zetten nu de stap om het daadwerkelijk te gaan implementeren", aldus Van der Vlugt. Hij benadrukt dat belangrijk is om in de eerste plaats een goede besturing te krijgen op dit contract dat een looptijd kent van tien jaar. Dit is ook aangehaald door het Bureau ICT-Toetsing (het BIT – sinds januari 2021 opgevolgd door het Adviescollege ICT toetsing), dat een blijvende rol zal houden bij GrIT in de uitvoeringsplannen.

Operator

GrIT bestaat uit 42 blokken. "Het eerste blok is de bouw van de nieuwe Twin datacenters en een uitwijklocatie. Dat is erg belangrijk voor ons, want daarmee creëren we de basis om de nieuwe IT op te gaan bouwen. De volgende blokken gaan we in opdracht geven en die hebben te maken met TITAAN, een 'moeilijke' afkorting voor onze operationele IT: *Theatre Independent Tactical Adaptive Armed Forces Network*. Dat is dus IT die we in het veld en aan boord van schepen gebruiken tijdens oefeningen en missies. Die is hard toe aan vernieuwing. Daarnaast maakt Defensie ook de belangrijke stap om een mobiele netwerk operator te worden. Dat heeft alles te maken met het feit dat wij dikwijls op locaties komen waar het netwerk van erkende providers er gewoon niet is. En op dat moment willen wij wel op een veilige en vertrouwde manier kunnen werken en niet afhankelijk zijn van een lokale provider. We kunnen écht daarmee onze beveiliging op een hoger niveau krijgen. Dat is cruciaal voor de belangrijke rol die wij hebben."

Van der Vlugt voorziet dat van de contractperiode van tien jaar de eerste zeven jaar wordt besteed aan bouwen. Hij glimlacht: "Ik hoor mensen denken 'Moet dat zo lang?', maar we zullen heus *agile* methodes toepassen in die periode. Waar het vooral om gaat, is dat we juist heel gefaseerd te werk gaan. Niet één grote waterval maar beheersbare blokken, zodat wij als Defensie daar ook gewoon goede sturing op kunnen hebben. Hoe ziet de wereld eruit over vijf, zes jaar? Ik weet het niet. Werken in een vrijwel leeg kantoor op anderhalve meter afstand van elkaar, dat hadden we begin vorig jaar ook niet kunnen bedenken. Vandaar dus de strategische keuze om het in blokken te implementeren."

De titel van Defensievisie 2035 is 'Vechten voor een veilige toekomst'. In de inleiding zegt demissionair minister Bijleveld dat gewapende conflicten maar ook handelsoorlogen, nepnieuws en cyberaanvallen Defensie dwingen tot vernieuwen.

"De Defensievisie 2035 beschrijft niet alleen de context van dreiging maar ook het antwoord dat we daarop willen geven. Het impliceert inderdaad een vernieuwing van onze Krijgsmacht. En dat betekent niet dat we gaan stoppen met varen en vliegen en met het rijden van voertuigen, maar dat er een heel nieuwe dimensie bijkomt en die dimensie heet 'cyberspace' of 'cyberwar'. Verder neemt ook de digitalisering van de traditionele wapensystemen een enorme vlucht. Een F35 is – om het heel oneerbiedig te zeggen – een vliegende datastofzuiger. Zo'n toestel haalt enorme hoeveelheden data binnen en met die data kun je vervolgens heel erg veel. Maar daar heb je wel de infrastructuur voor nodig, want heb je die niet, dan ben je niet voorbereid op die toekomst. Daarom is GrIT ook zo belangrijk. Onze huidige infrastructuur is prima geschikt voor het huidige werk dat wij doen, maar naar de toekomst toe hebben wij die nieuwe functionaliteiten absoluut nodig."

Cyber

'Cyber' moet naar een hoger niveau, stelt Van der Vlugt. "Wat je ziet is dat de aard van het conflict aan het veranderen is. Je ziet tegenwoordig vaak eerst dat er bijvoorbeeld met informatiecampagnes, desinformatiecampagnes moet ik zeggen, geprobeerd wordt om de publieke opinie te beïnvloeden. Dat gaat gewoon via openbare kanalen als Facebook, Twitter etcetera. *Fake news*, wat is waar en wat is niet waar?, dat is heel erg lastig om onderscheid in te maken. En wat je in toenemende mate ziet zijn *deep fakes*: er wordt een filmpje van jou opgenomen, iemand plakt daar een andere tekst in, en de computer animeert dat op een dusdanige manier dat het niet meer duidelijk is wat jij nu daadwerkelijk zegt. Dus die desinformatie, daar begint het vaak mee in die campagnes. Wat je vervolgens ziet, is dat die landen – die worden met een mooie term ook wel 'statelijke actoren' genoemd – veel harder gaan ingrijpen in het cyberdomein. Ze proberen om vitale infrastructuur – denk aan telefonie, aan energie – te beïnvloeden of zelfs zodanig te verstoren, dat het niet meer functioneert. Dat hebben we gezien in de Oekraïne, dat hebben we gezien in de Baltische Staten. En de volgende stap is dat de traditionele oorlogsvoering binnen komt. Dat hebben we op de Krim gezien: eerst die desinformatie, toen die cyberaanvallen en vervolgens kwam Rusland met '*little green men*' de grens over."

Andersom zit ook de westerse wereld niet stil, erkent Van der Vlugt, denk aan Irak en Afghanistan. "Maar mijn scope, mijn verantwoordelijkheid, ligt niet bij de offensieve kant van cyber, maar bij de defensieve: onze digitale weerbaarheid.

Tegelijkertijd, in het militaire domein, zien we natuurlijk wel de ontwikkeling van dat soort *capabilities* en daar hebben wij ook gesprekken over. Daar zitten ook allerlei ethische dilemma's die we goed met elkaar moeten afwegen. Dat doen we niet alleen als Nederland, dat doen we ook in internationaal verband met onze partners."

Hij noemt de inlichtingendiensten MIVD en AIVD[1] (“Die zijn onze ogen en oren in het cyberdomein”), de Nationale Politie (“Een belangrijke partner op het gebied van *high tech crime*”), de NCTV en NCSC[2] en het ministerie van Justitie en Veiligheid als primaire bondgenoten. “Cyber is een gezamenlijke verantwoordelijkheid van de BV Nederland en ik hoop ook echt dat we straks, na de Tweede Kamer verkiezingen, in het nieuwe Regeerakkoord terugzien dat cyber een belangrijkere positie krijgt. We moeten ons afvragen in welke mate we autonomie willen hebben op onze eigen (NL) netwerken. Nederland is één van de landen met het hoogste aantal internetaansluitingen, maar dat maakt ons ook kwetsbaar want daar kunnen kwaadwillende partijen, of dat nou landen zijn of criminelen, in potentie misbruik van maken. Dus hoe gaan we ons daartegen bewapenen, moeten we voor noodsituaties bijvoorbeeld een eigen (internet) netwerk hebben? Defensie beschikt over een eigen netwerk voor haar eigen IT en dat biedt ons veel voordelen voor de beveiliging, dat hoef ik denk ik niet uit te leggen. We moeten niet naïef zijn in wat er om ons heen gebeurt.”

Data science

“Ik heb een warm hart voor data en data science”, zegt Van der Vlugt. “Ik geloof echt dat ten aanzien van digitalisering van de Krijgsmacht, informatiegestuurd optreden heel cruciaal is voor de volgende stap. De ontwikkelingen gaan snel, de BV Nederland doet het op het gebied van data science goed. Een aantal grote bedrijven is heel succesvol, denk aan Ayden en Booking.com. Ik besteed veel tijd en aandacht aan het vergroten van onze *data awareness*, omdat ik echt geloof dat data science een *game changer* gaat worden. Vanwege het feit dat data een enorme boost geeft aan onze digitalisering. En onder data science versta ik ook technologieën als AI en *machine learning*. Tegelijkertijd moeten we dat datagebruik wel op een zorgvuldige en ethische wijze organiseren.”

“IT is als water uit de kraan: we kunnen niet meer zonder en het moet er 24x7x365 dagen zijn. Wij zijn zó afhankelijk van onze IT geworden, net zoals alle grote bedrijven. Daarom stellen we ook hoge eisen en randvoorwaarden aan onze infrastructuur om dat te operationaliseren, vandaar ook het contract Grensverleggende IT.”

Een ander omvangrijk programma betreft FOXTROT. “Dat is voor ons mobiele domein, het vernieuwen van de IT-infrastructuur aan boord van voertuigen bijvoorbeeld. Ook dat is voor ons heel cruciaal. Wij opereren in specifieke omstandigheden, op het moment dat wij in Afghanistan of ergens anders ter wereld de poort uit rijden, kunnen we niet zo maar even gebruik maken van de plaatselijke 4G- of 5G-netwerken. Satellietcommunicatie is onder sommige omstandigheden ook niet mogelijk, omdat je bijvoorbeeld niet opgemerkt wil worden. Dus je bent daar in je interoperabiliteit ook sterk afhankelijk van andere vormen van communicatie en al die apparatuur moet daar ook daadwerkelijk geschikt voor zijn.”

Van der Vlugt merkt op “heel blij” te zijn met het advies van het Bureau ICT-Toetsing. “Zij houden ons een goede spiegel voor over hoe zij naar de situatie kijken, vanuit hun kennis en ervaring. Dat heeft ertoe geleid dat we het programma op een heel andere manier hebben ingericht. Ik denk dat dit echt winst is en ik ben ook blij dat zij meekijken naar de verschillende uitvoeringsplannen die wij gaan maken, dat zie ik echt als toegevoegde waarde.” Van der Vlugt zegt dat ook de besturing op IT-projecten is herzien en op een andere manier ingericht. IT, data en cyber worden geagendeerd binnen de bestuursraad van Defensie onder een ‘stuurgroep digitale transformatie’. De bestuursraad is het hoogste gremium binnen het departement. Ook is Defensie bezig met de inrichting van een eigen CIO-stelsel. Dit impliceert de komst van decentrale CIO’s binnen de Landmacht, Luchtmacht, Marine en andere Defensieonderdelen.

[1] MIVD = Militaire Inlichtingen- en Veiligheidsdienst, AIVD = Algemene Inlichtingen- en Veiligheidsdienst

[2] NCTV = Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCSC = Nationaal Cyber Security Centrum