



Dat de digitalisering doorzet bewijst onder meer de F-35, een vliegende 'datastofzuiger' die vol zit met technologie

FOTO MCD, JAN DIJKSTRA

Het versterken van warfighting capabilities door digitalisering

Commandeur b.d. Peter van den Berg

Dr. ir. Michiel Borgers

Brigade-generaal Aard Lettink

Ir. Rob Schepens*

Drones, cyberaanvallen, ontploffende piepers, unmanned vehicles, desinformatie: de digitalisering in het militaire conflict neemt steeds verder toe en zou zomaar in een toekomstig conflict het verschil kunnen maken. Hoe kan Defensie in een gewapend conflict doeltreffender optreden door de inzet van IT? Op basis van een analyse van recente conflicten geeft dit artikel een overzicht van *warfighting capabilities* en hoe de digitalisering die capability heeft verbeterd. Welke warfighting capabilities zijn in het gevecht essentieel en hoe kan digitalisering die versterken?

* Cdr b.d. Peter van den Berg is strategisch adviseur IT bij CZSK; dr. ir. Michiel Borgers is directeur JIVC (het IT-bedrijf van Defensie); brigade-generaal Aard Lettink is decentrale Chief Information Officer bij de Koninklijke Marchaussee; ir. Rob Schepens is decentrale Chief Information Officer bij de Bestuursstaf van Defensie.

1 Digitalisering: wanneer data uit de hele organisatie en haar omgeving worden verwerkt met behulp van geavanceerde digitale technologieën, wat leidt tot fundamentele veranderingen in bedrijfsprocessen die kunnen leiden tot nieuwe bedrijfsmodellen en sociale veranderingen.

Digitalisering van het gevecht

Digitalisering,¹ als instrument om doelen te bereiken door middel van technologische innovaties en digitale transformaties, heeft op veel plekken in de maatschappij voor een fundamentele verandering gezorgd. Voorbeelden hiervan zijn Airbnb in de recreatiesector, het

thuiswerken met *video conferencing* en de cryptovaluta en digitaal bankieren in de banksector. Op het militaire vlak is deze fundamentele verandering ook al in gang gezet. De traditionele manier van oorlogvoering wordt gecombineerd met de inzet van (digitale) technologieën om het beoogde effect te realiseren. De adequate inzet van gedigitaliseerde warfighting capabilities² is daarmee van cruciaal belang voor de militair om succesvol te zijn in het conflict. Recente conflicten worden gekenmerkt door de inzet van veel nieuwe technologie, maar kijkend naar de mogelijkheden van AI en quantum-technologie is de verwachting dat de digitalisering een nog grotere impact zal hebben.

Sinds de grootschalige inval van Rusland in Oekraïne op 24 februari 2022 is een verandering in het gevecht zichtbaar geworden. Meerdere (gewapende) conflicten in een breed geopolitiek spectrum hebben elkaar in hoog tempo opgevolgd, met een paradigmaverschuiving van pure kinetische oorlogvoering naar het hybride gevecht. Het gevecht wordt meer en meer gevoerd in het digitale domein. Het fysieke domein kent de inzet van grote hoeveelheden drones en onbemande voertuigen, dit alles ondersteund door de inzet van AI. Op het slagveld van Oekraïne worden nieuwe technologieën in snel tempo geïntroduceerd, uitgetest en verbeterd.

Digitalisering als multiplier

Uit de geschiedenis blijkt dat er bij elk gewapend conflict een versnelling in de technologische ontwikkeling plaatsvindt. De opkomst van computers tot en met het ontdekken van nieuwe ruimtetechnologieën zijn hier voorbeelden van. In de Tweede Wereldoorlog zorgde de computer, onder meer ontwikkeld door Alan Turing, er voor dat met de Enigma gecodeerde berichten van de Duitsers ontcijferd konden worden. Dit zou er zelfs voor gezorgd hebben dat de geallieerden uiteindelijk zouden overwinnen.³ Deze nieuw ontwikkelde computer zorgde voor de juiste informatiepositie en verbetering van wat tegenwoordig Informatiegestuurd Optreden wordt genoemd.⁴ De technologische ontwikkelingen hebben sinds de Tweede Wereldoorlog niet stilgestaan. De toepassing en de integratie

van IT in allerlei defensiematerieel is steeds groter geworden, dan wel onmisbaar. Duidelijke voorbeelden hiervan zijn de Reaper en de F-35, die gezien kunnen worden als vliegende 'datastofzuigers' en vol zitten met allerlei technologie.

Defensie wil uiteraard ook doeltreffender kunnen optreden in het militaire domein. De digitalisering zoals in de eerste paragraaf beschreven dient gericht te zijn op de warfighting capabilities die in het kader van hoofdtak 1 relevant zijn.

Hierna komen die warfighting capabilities aan bod, gezien vanuit het Defensie Capability-model. Daarna wordt, op basis van recente conflicten, gekeken welke warfighting capabilities Defensie met behulp van digitalisering moet versterken.

Warfighting capabilities

Een Defensie Capability-model is een handig instrument bij het beschrijven en analyseren wat een organisatie kan of zou moeten kunnen doen. Of nauwkeuriger: business capabilities zijn de vaardigheden of functies die een organisatie heeft of zou moeten hebben om haar doelen te bereiken. Een business capability omvat de mensen, processen, informatie en middelen van de organisatie.⁵ Door de capabilities inzichtelijk te maken, ten opzichte van elkaar te ordenen en te waarderen, kan een organisatie eenvoudiger weloverwogen beslissingen nemen over prioriteiten en daarbij behorende investeringen. Welke capabilities heeft Defensie nodig om klaar te zijn voor het gevecht?

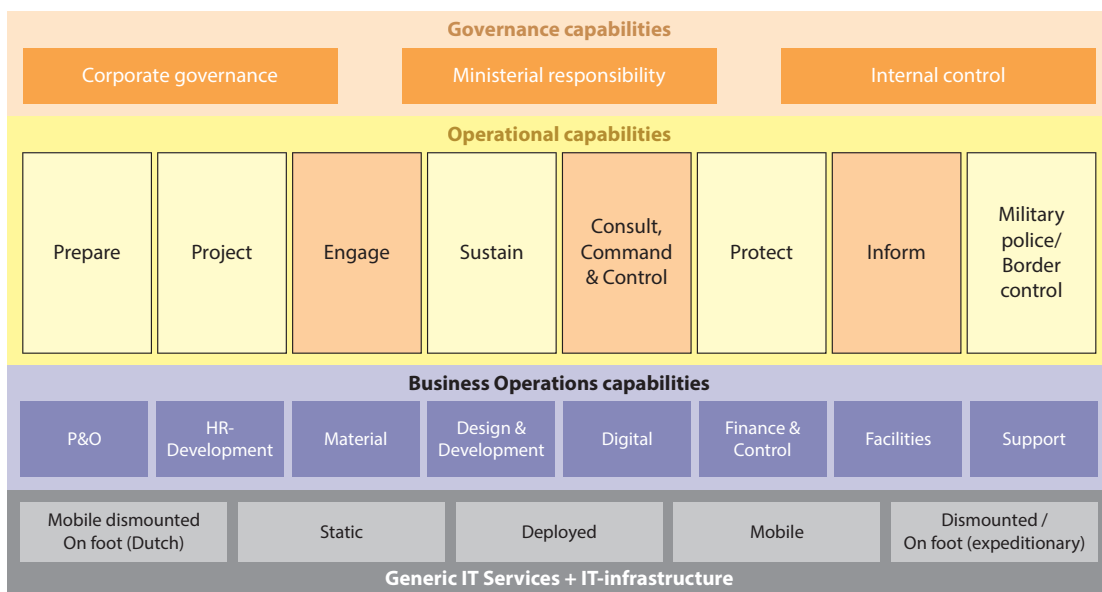
De Nederlandse defensieorganisatie heeft haar business capabilities eveneens in een zogeheten

2 Warfighting capability: een militaire functie die een defensieorganisatie nodig heeft in het gevecht.

3 Zie voor meer informatie over de Enigma-codeermachine: [https://nl.wikipedia.org/wiki/Enigma_\(codeermachine\)](https://nl.wikipedia.org/wiki/Enigma_(codeermachine)).

4 Beleidsvisie Informatiegestuurd Optreden. Sneller, slimmer, sterker (Den Haag, ministerie van Defensie, 4 juli 2023).

5 TOGAF Business Capabilities Guide V2. Zie: https://pubs.opengroup.org/togaf-standard/business-architecture/business-capabilities.html?utm_source=chatgpt.com.



Figuur 1 Het Defensie capability-model

capability model geplaatst, waarbij als basis gebruik is gemaakt van het capability model van de NAVO. In het model wordt een onderscheid gemaakt in besturende, bedrijfsvoerings- en operationele capabilities (zie figuur 1). De operationele capabilities zijn functies die specifiek zijn voor de defensieorganisatie. De operationele capabilities behelzen functies, zoals 'Prepare' en 'Consult, Command & Control'. De eerste functie omvat onder andere de personele- en materiële gereedstelling, terwijl onder de tweede de commandovoering is terug te vinden. Dus als het om warfighting capabilities gaat, dan gaat het over de operationele capabilities van Defensie.

Digitalisering van de warfighting capabilities

Door de teruglopende defensiebegrotingen vanaf 2011 is er sinds die tijd ook structureel te weinig geïnvesteerd in IT. Daardoor kon het IT-landschap niet meegroeien met haar tijd en bleef de digitalisering van de warfighting capabilities achter. Vanaf 2015 zijn er wel investeringen gedaan in een aantal grote programma's om de

achterstand in te halen,⁶ maar grote programma's worden meestal niet gekenmerkt door snelle resultaten.

In 2025 heeft de defensieorganisatie een herijking gedaan van haar IT-portfolio om meer focus aan te brengen in de veelheid van projecten. Met deze herijking richt Defensie het realisatievermogen op de meest essentiële warfighting capabilities. Deze ingreep zal ervoor zorgen dat er meer water uit de IT-kraan komt. Voor deze herijking is op basis van het capability model gekeken naar de capabilities die vanuit digitalisering prioriteit zouden moeten krijgen in het kader van het uitvoeren van hoofdtak 1. Daarnaast is gekeken welke van deze capabilities nog onvoldoende of geen IT-ondersteuning hebben gehad. Hierbij kan gedacht worden aan het op orde krijgen van de internationale interoperabiliteit via de FMN-standaarden⁷ of het versterken van de *situational awareness* en *situational understanding*. Uit die analyse komt naar voren dat er nog over een breed gebied van capabilities geïnvesteerd moet worden. Door die noodzaak aan investeringen in digitalisering blijft het risico dat Defensie te weinig snelheid maakt. Om in het gevecht echt het verschil te maken, is een aanscherping van de prioriteiten

⁶ Ministerie van Defensie 2 H Definitief v1.0.

⁷ What is the NATO Warfighting Capstone Concept? Zie: <https://www.act.nato.int/activities/federated-mission-networking/>.

wenselijk. Hierna zoomt dit artikel daarom eerst in op de digitalisering zoals deze is toegepast in recente conflicten. De praktijk geeft dan mogelijk extra richting aan welke warfighting capabilities het belangrijkst zijn om te versterken.

Digitalisering in recente conflicten

Als het gaat om warfighting capabilities dan is het interessant om te bekijken hoe digitalisering in een aantal recente gewapende conflicten is ingezet. Zowel in de Oekraïne-oorlog als ook in het Midden-Oosten heeft digitalisering op een aantal terreinen een vlucht genomen. Deze zijn te groeperen naar vier trends.

1 Offensieve cyberoorlogvoering

Bij cyberoorlogvoering gaat het om het verstoren van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Oftewel, offensieve cyberoorlogsvoering is gericht op het beïnvloeden, verstoren of vernietigen van informatie en informatiesystemen van tegenstanders. Deze operaties kunnen variëren van het verzamelen van inlichtingen tot het uitvoeren van aanvallen die fysieke effecten hebben, zoals het uitschakelen van kritieke infrastructuur.⁸ Een concreet voorbeeld hiervan is het door de Verenigde Staten uitschakelen van de stroom in Venezuela bij het ontvoeren van president Maduro.

Rusland voerde, ruim voor de inval in 2022, al digitale aanvallen uit op het elektriciteitsnetwerk en het fiscale systeem van Oekraïne in respectievelijk 2015-2016 en 2017.⁹ Ook in het conflict tussen Israël en Hamas heeft allerlei cyberoorlogvoering plaats gevonden, zoals de DDos-aanvallen (Distributed Denial-of-Service) van Hamas op Israëlische organisaties.¹⁰ Kijkend naar het capability model, komt offensieve cyberoorlogvoering terug bij veel van de operationele capabilities waar de nadruk ligt op Engage en Inform. Het kan zorgen voor een effect in het fysieke, virtuele of het cognitieve domein.¹¹

2 Intel-to-shooter

Om de vijand succesvol te kunnen aanvallen moet het tijdsverloop tussen doeldetectie en 'wapen op doel' zo kort mogelijk zijn. Inlichtingen dienen snel en efficiënt gebruikt te worden om een doelwit te lokaliseren. Dit kunnen vijandelijke posities, militaire activiteit of bepaalde grondbewegingen zijn die via middelen zoals drones, radar, satellieten of menselijke waarnemingen worden opgevangen.^{12,13} De inlichtingen dienen real-time verwerkt en gedeeld te worden met de shooter: van de gevechtsvlieger tot aan de drone-operator. De oorlog in Oekraïne laat dagelijks het belang van het concept *intel-to-shooter* zien, waarbij op allerlei manieren doelinformatie wordt vergaard en verwerkt, zowel op tactisch als op strategisch niveau.

Innovatieve ontwikkelingen op het gebied van C4ISR (Command, Control, Communication & Computers, Intelligence, Surveillance en Reconnaissance) zorgen ervoor dat informatie en aanvals- en verdedigingsopdrachten vrijwel direct worden gedeeld met de juiste eenheden. Naast deze (*near*) *real-time* samenwerking is nauwkeurigheid bepalend voor het succesvol onder vuur nemen van doelen of juist het ontwijken van vijandelijk vuur. Met deze ontwikkeling worden vooral de capabilities Engage, Consult, Command & Control en Inform versterkt.

3. Situational awareness en situational understanding

In meerdere recente conflicten wordt geprobeerd om informatie uit allerlei publieke en private bronnen te verzamelen en te combineren om zo te zorgen voor *situational awareness* en *situational*

8 P.A.L. Ducheine, 'Je hoeft geen zwaard en schild te dragen om ridder te zijn', *Militaire Spectator* 185 (2016) (3) 123-135.

9 K. Arnold, P. Pijpers en P. Schrijver, 'Assessing the Dogs of Cyberwar. Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War', in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024) 231-256.

10 Omer Yoachimik en Jorge Pacheco, 'Cyber attacks in the Israel-Hamas War' (23 oktober 2023). Zie: https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/?utm_source=chatgpt.com/.

11 H. van Beek en S. Rietjens, 'Open-Source Intelligence in the Russia-Ukraine War' in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024).

12 L. Peperkamp en P. Bolder, 'The Space Domain and the Russia-Ukraine War', in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024).

13 Delta (situational awareness system). Zie: [https://en.wikipedia.org/wiki/Delta_\(situational_awareness_system\)](https://en.wikipedia.org/wiki/Delta_(situational_awareness_system)).



Een Oekraïense drone-operator monteert een Starlink-communicatiesysteem. Oekraïense eenheden passen hun drones real-time aan aan veranderende electronic warfare-omstandigheden op het gevechtveld

understanding. Deze wordt vervolgens gebruikt om tot een Common Operational Picture te komen en de strategie daarop aan te passen. Oekraïne heeft met zijn Delta-systeem zijn situational awareness vergroot en heeft deze gekoppeld aan zijn Battlefield Management Systeem. Deze trend kan het best gezien worden als wat bij Defensie Informatiegestuurd Optreden wordt genoemd en raakt in de kern de capabilities Consult, Command & Control en Inform.

4 Drones en (semi-)autonome systemen

De toepassing van (semi-)autonome systemen bij gewapende conflicten is niet meer weg te denken. Voorbeelden van militaire (semi-)autonome systemen die we op het slagveld van Oekraïne tegenkomen zijn bewapende drones (UAV's), robotica voor mijndetectie en opruiming, zelfrijdende en -varende wapendragers en verdedigingssystemen die zelfstandig detecteren en onderscheppen. De technologie achter deze systemen heeft een grote vlucht genomen, waarbij de effectiviteit door de introductie van AI aanzienlijk is verbeterd. Tegenwoordig wordt het concept van *human-in-the-loop* steeds meer losgelaten en nemen de systemen autonoom

beslissingen zoals het identificeren van vijandelijke doelen of het afvuren van wapens. Vanuit de recente conflicten hebben Israël en ook Oekraïne en Rusland aanzienlijke stappen gezet in de ontwikkeling en inzet van autonome en onbemande systemen. Er is op dit moment nog geen publiek beschikbare informatie die bevestigt dat deze landen gevechten uitvoeren met bijna uitsluitend autonome systemen. De integratie van deze technologieën lijkt momenteel vooral complementair te zijn aan traditionele militaire operaties. De inzet van (semi-)autonome systemen richt zich op de Engage- capability.

Delta

De vier bovenstaande trends laten zien dat digitalisering vooral effect heeft op drie warfighting capabilities: Engage, Consult, Command & Control en Inform, zoals die in figuur 1 terug zijn te vinden. Als Defensie haar warfighting capabilities wil versterken met digitalisering dan zouden deze drie capabilities in ieder geval aandacht moeten krijgen. Daarbij is het interessant om te zien dat de Inform-capability een belangrijke rol speelt ter ondersteuning van de andere twee. Want zonder

informatie – en daarmee de ondersteuning van digitalisering – is geen enkele capability goed uit te voeren. Om dit concreet te maken kan het Delta-systeem uit Oekraïne als voorbeeld gelden. Delta is zowel een situational awareness- als een Battle Management System dat door de Oekraïense Defensie ontwikkeld is. De kracht van het systeem is dat het uit een grote diversiteit aan bronnen informatie verzamelt, zoals satellietbeelden, drones, inlichtingen en geo-informatie. Delta wordt gebruikt voor het plannen van operaties, coördinatie en informatievoorziening.¹¹ Met het Delta-systeem heeft Oekraïne daarmee niet alleen zijn Inform-capability versterkt, maar ook de Consult, Command & Control en Engage-capabilities. Deze betere informatiepositie is een van de redenen waarom Oekraïne nog steeds standhoudt tegen een kwantitatief veel grotere tegenstander.

Conclusies en vervolg

De wereld van oorlogvoering is aan het veranderen. De digitalisering zorgt er voor dat het

gevecht andere vormen aanneemt. Om Defensie daarop voor te bereiden is in dit artikel gekeken naar hoe de Nederlandse warfighting capabilities kunnen worden versterkt met digitalisering. Recente conflicten – en de oorlog in Oekraïne in het bijzonder – tonen aan dat er drie capabilities zijn die Defensie met digitalisering kan versterken: Engage, Consult, Command & Control en Inform. Op de juiste manier ingezet kan digitalisering het verschil maken in het gevecht.

Als Defensie hierop wil versnellen zal de organisatie moeten transformeren naar andere manieren van voortbrenging en levering van IT. De Digitale Transformatie Strategie, en het multi-modaal werken daarbinnen, gaat zorgen voor die versnelling. In ieder geval luidt de conclusie dat Defensie met urgentie de digitalisering zal moeten oppakken als zij in de afschrikking en in een gewapend conflict het verschil wil maken. Hierbij is het werken met capabilities het vertrekpunt. De uiteindelijke winst van de digitale transformatie is immers een grotere gevechtskracht. ■



FOTO ANP/APR SERGEJ STOEPINSKI

Zonder informatie – en daarmee de ondersteuning van digitalisering – is geen enkele capability goed uit te voeren. Om dit concreet te maken kan Defensie het Delta-systeem uit Oekraïne als voorbeeld nemen