

# NetForce: een nieuw model voor toekomstige Defensie

## *‘Unleash the Power of the Netted Force’*

**‘Revolutions in military affairs’ (RMA) vallen altijd samen met belangrijke ideologische, culturele of technologische vernieuwingen. Het resultaat hiervan is een significante verandering in de manier van oorlogvoering. Onze huidige hyperconnectieve wereld, waarin dreigingen direct de nationale veiligheid beïnvloeden, vergt een nieuwe oriëntatie op ‘Defensie’. Als basismodel voor de toekomstige krijgsmacht stelt dit artikel een netwerkorganisatie voor met een verregaande vorm van zelfsturing. Dit model, NetForce genaamd, baseert zich op de mogelijkheden die mondiale hyperconnectiviteit bieden. De complexiteit, fluiditeit, dynamiek en wereldwijde verwevenheid van hedendaagse conflicten enerzijds en het behendige en innovatieve optreden van tegenstanders anderzijds – in combinatie met de beperkte houdbaarheid van het huidige organisatiemodel en het beperkte succes van recente NAVO-operaties – geven voldoende redenen om het NetForce gedachtegoed te verkennen en verder te onderzoeken.**

*Kolonel J.A. van Dalen, luitenant-kolonel P.A.P. Dekkers en luitenant-kolonel A.F. van Daalen\**

Een gewaarschuwd lezer telt voor twee. Dit artikel gaat namelijk over een toekomstige vorm van inzet van militair vermogen. Een nieuwe vorm, die een trendbreuk betekent met gangbare militaire opvattingen en dus niet zonder meer aansluit bij traditioneel militair denken. Dit artikel gaat dus niet over hiërarchische verbanden, commanderen en controle, maar over zijwaartse verbindingen, synchroniseren en zelforganisatie. Dit artikel gaat, kortom, over NetForce.

We bouwen het artikel als volgt op. Eerst leggen we uit waarom er nieuwe inzetvormen van militair vermogen komen, of we dit nu willen of niet. Deze nieuwe inzetvormen noemen we NetForce. Daarna beschrijven we

wat we onder NetForce verstaan en leggen uit waarom het een beter antwoord biedt op genetwerkte of hybride tegenstanders dan de huidige organisatievorm.

Nadat we aldus de basisgedachten hebben uitgelegd, gaan we NetForce meer in detail behandelen. De nadruk ligt daarbij op de bijbehorende functies van NetForce optreden en organisatie. Vervolgens gaan we in op

\* Kolonel J. A. (Hans) van Dalen EMSD is commandant Joint ISTAR Commando. Lkol P.A.P. (Patrick) Dekkers MSSM EMSD is werkzaam als afdelingshoofd bij het Nationaal Cyber-Security Centrum van de Nationaal Coördinator voor Terrorismebestrijding en Veiligheid. Lkol A.F. (Arjan) van Daalen werkt voor het bureau Trends & Concepts van het Land Warfare Centre. De schrijvers danken lkol J. van Esch, ritm K. van Oort en kol R. van Harskamp voor hun opbouwende kritiek.

FOTO MCD, E.J. DANIELS



Elk tijdperk kent zijn eigen vorm van oorlogvoering. De tank is ontwikkeld om mobiliteit, bescherming en vuurkracht te combineren, en heeft daarmee het paard verdrongen

vernieuwingen, en resulteren dan ook veelal in aanzienlijke veranderingen in de manier van oorlogvoering. Vernieuwingen bieden immers kansen.

Enkele voorbeelden ter illustratie. Manoeuvre-oorlogvoering heeft het concept belegeringen verdrongen. De tank is ontwikkeld om mobiliteit, bescherming en vuurkracht te combineren, en heeft daarmee het paard verdrongen. Andere ontwikkelingen die de wijze van oorlogvoering aanzienlijk hebben aangepast, zijn het gebruik van grootschalig indirect vuur, de invoering van het operationele niveau, de introductie van de mitrailleur, het gebruik van de derde dimensie, *subsurface-warfare* en massavernietigingswapens.

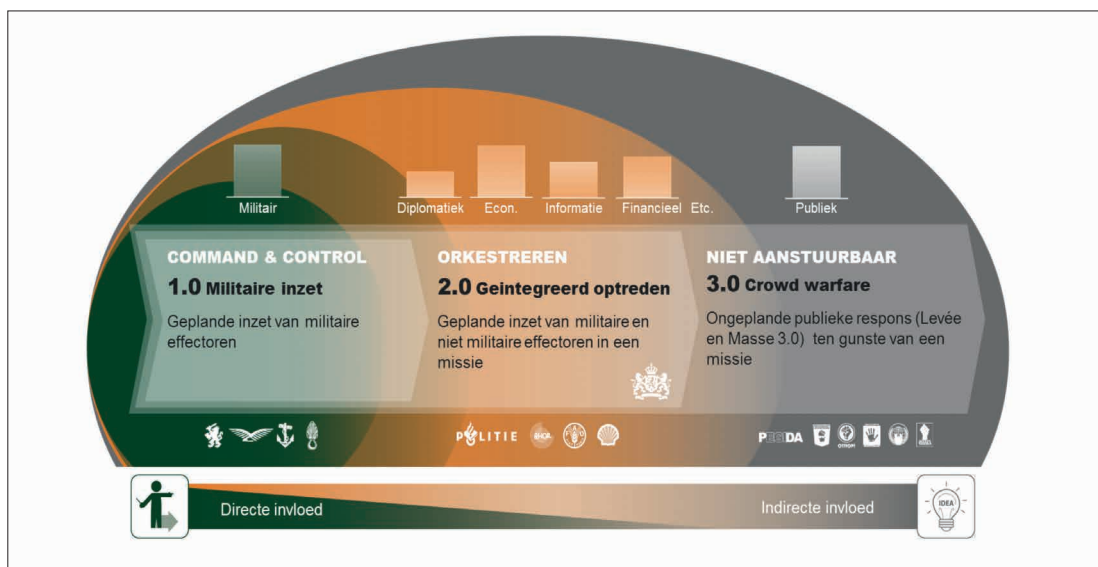
sterkten en zwakten van een dergelijke vorm van optreden. We sluiten af met enkele bespiegelende opmerkingen.

### Waarom een nieuwe vorm van militair vermogen?

Zoals Von Clausewitz al stelde kent elk tijdperk zijn eigen vorm van oorlogvoering. Veranderingen van tijdperken vallen samen met belangrijke ideologische, culturele of technologische

Kenmerkend is het gebruik van nieuwe ontwikkelingen en innovatieve wijze van optreden om de geijkte organisaties en methodieken (bij de tegenstander) te omzeilen, zodat de beoogde doelstellingen effectief worden bereikt. Niet openstaan voor dergelijke innovaties heeft menig krijgsmacht en staat de kop gekost.

Een bruikbaar kader om veranderingen in de manier van oorlogvoering als gevolg van wetenschappelijke vooruitgang inzichtelijk te maken levert Antoine J. Bousquet.<sup>1</sup> Hij schetst



Figuur 1 Mate van aanstuurbaarheid en invloed in operaties



FOTO: US ARMY, P. WALZ

In de cybernetische manier van oorlogvoering draait alles om informatiebeheersing en rekenkracht van computers. Deze manier van oorlogvoering heet NetCentric Warfare en werd geperfectioneerd door de Amerikaanse eenheden tijdens de beide Golfoorlogen

aan de hand van metaforen vier belangrijke wetenschappelijke veranderingen en dienvolgt ook vier manieren van oorlogvoering.

#### **Metafoor: klok**

De eerste grote verandering van oorlogvoering werd veroorzaakt door de perfectionering van mechanische constructies (metafoor: klok). Dit leidde tot het inzicht dat oorlogvoering draaide om voorbereiding, discipline en orde, zoals geperfectioneerd door de legers van Frederik de Grote en Napoleon.

#### **Metafoor: verbrandingsmotor**

Dit inzicht werd echter teniet gedaan door het benutten van fossiele brandstoffen voor energie bij oorlogvoering (metafoor: verbrandingsmotor). Deze factor leidde tot een thermodynamische manier van oorlogvoering, waarbij alles draaide om vernietigingskracht. Dit culmineerde in de ongekende vernietigingen tijdens de beide wereldoorlogen, geïllustreerd door kracht van de Duitse Blitzkrieg.

#### **Metafoor: computer**

Een derde belangrijk technologische uitvinding was de computer (metafoor: computer). In die cybernetische manier van oorlogvoering draait alles om informatiebeheersing en rekenkracht van computers. Deze manier van oorlogvoering werd geperfectioneerd door de Amerikaanse eenheden tijdens de beide Golfoorlogen en vastgelegd in de Air Land Battle Doctrine. De partij die het beste in staat was om zoveel mogelijk omgevingsinformatie te verzamelen zou conflicten in haar voordeel beslissen. Dit werd ook wel NetCentric Warfare genoemd.

De continue drang naar méér en betere informatie verlamde de besluitvorming echter, en verminderde bovendien het reactievermogen van militaire eenheden. Ook nu vindt een dergelijke belangrijke tijdperkverandering

1 Bousquet, A.J., *The Scientific Way of Warfare, Order and Chaos on the Battlefield of Modernity*, London, 2009.

plaats. De vierde ontwikkeling is namelijk hyperconnectiviteit.<sup>2</sup> De introductie van de computer en internet heeft immers geleid tot een 'informatierevolutie,' globale transparantie en een ongekende wereldwijde onderlinge verbondenheid.

### Metafoor: ecosysteem

Deze ontwikkeling resulteert in veel positieve maar ook disruptieve veranderingen, die vaak razendsnel plaatsvinden en alle aspecten van moderne samenlevingen raken. Er is sprake van een wereldwijde snelle verspreiding van kennis, maar ook van een complexe, dynamische en fluïde veiligheidsomgeving, met een veelvoud van actoren en factoren die op elkaar inwerken (metafoor: ecosysteem). De partij die het beste met deze omstandigheden kan omgaan, zal de bovenliggende partij blijken.

Naar onze mening kan een dergelijke tijdperkverandering niet worden tegengehouden. We betogen daarom dat onze traditionele militaire organisatievorm, gebaseerd op hiërarchie en controle, moet kunnen meebewegen met de mogelijkheden die de omgeving biedt. Stoicijns blijven vasthouden aan één vorm van organiseren werkt niet. Niet meeveranderen betekent immers uiteindelijk verlies van relevantie en/of succes: opponenten benutten

de kansen die de tijdperkverandering biedt eerder. We hebben dus een nieuwe vorm van inzet van (militair) vermogen nodig.

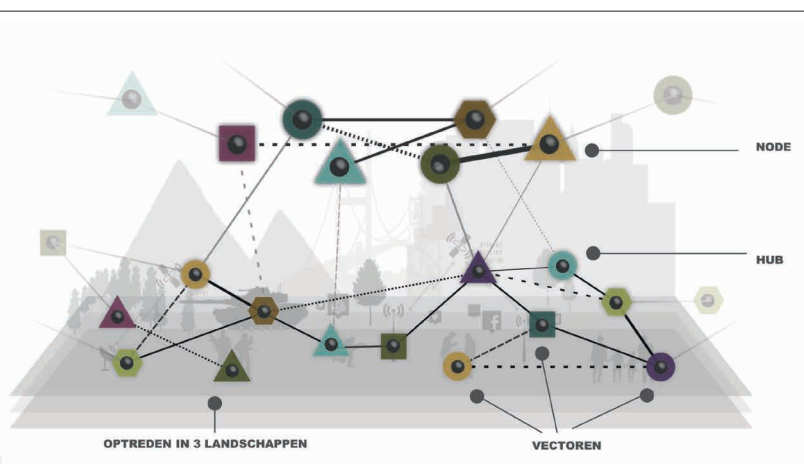
## Wat gaat er veranderen?

Wat gaat er nu eigenlijk precies veranderen aan het militair vermogen in het informatietijdperk? Traditionele militaire hiërarchie heeft altijd gewerkt, omdat ze een functie vervulde, namelijk het bieden van overzicht en aanvullende instructies voor eenheden te veld in het strijdgevoel. Van commandanten die op heuvels met een verrekijker de veldslag gadesloegen en met seiners en trommelaars probeerden bij te sturen, tot de *reports & returns* systematiek die we nu kennen.

Hiërarchische niveaus waren dus nodig om grotere eenheden en verbanden aan te sturen. Het kon fysiek immers ook niet anders. Maar in het razendsnelle informatietijdperk, dat ons nog grotendeels te wachten staat, werkt dit tegen ons. De veelvoud van commandolagen (gebaseerd op een voor een commandant behapbare *span of control*) is namelijk niet snel genoeg in staat om te kunnen inspelen op de dynamische en complexe omgeving. Denk hierbij aan de sneeuwballijsten en telefoonkettingen om te kunnen mobiliseren van nog niet zo lang geleden, die veel tijd in beslag namen en zeker niet garandeerden dat een bericht probleemloos aankwam.

Tegenwoordig mobiliseren we met één *WhatsApp*-bericht complete brigades, zonder vertraging en met onverminderde informatie. Korporaal en generaal kunnen gelijktijdig over dezelfde informatiestand beschikken; de interpretatie en het nut van de informatie is voor beiden uiteraard anders.

Tegelijkertijd is dit fenomeen natuurlijk niet voorbehouden aan militaire eenheden of staten. Een zestienjarige hacker in Maleisië kan een formidabele tegenstander worden. Hij kan bijvoorbeeld complete logistieke ketens, hoofdkwartieren of vlootverbanden ontwrichten. Ieder individu kan tegenwoordig netwerken opzetten, snel mobiliseren en



Figuur 2 Abstracte weergave van NetForce

<sup>2</sup> Dekkers, P.A.P., Van Daalen, J.A., Van de Boor, R., *Operating Concept Ascalon*, LWC, 2016.

anderen informeren, *empowered* door informatie-technologie. Hiermee kan dus (militair) vermogen worden gegenereerd, en daarmee macht om daadwerkelijk te interveniëren in een conflict.

Dit fenomeen duiden we aan met de termen *crowd warfare* oftewel *Levée en Masse électronique*<sup>3</sup>, waarbij netwerken en individuen, geïnspireerd door een idee, zich verenigen. Prille varianten zijn bewegingen als Occupy, Otpor, Pegida, Anonymous. Hun succes is wisselend, maar dit soort bewegingen zijn wel voorbodes van wat ons te wachten staat en kunnen veel krachtiger worden.

Gewapend kan ook, denk aan het wereldwijd rekruteren en aansturen van jihadisten, zoals ISIS en al-Qaida succesvol doen. Zo ontstaan moeilijk doordringbare tegenstanders, die zichzelf in stand houden en wereldwijd opereren. Stelt u zich eens voor hoe deze ontwikkeling zich kan voortzetten in pakweg tien tot twintig jaar! Gebruikmaken van de mogelijkheden die informatietechnologie ons biedt, geeft dus nieuwe kansen en bedreigingen die het gebruik van militair vermogen fundamenteel zullen veranderen. NetForce beoogt deze kansen te benutten om hiermee tegelijkertijd bedreigingen te kunnen afwenden.

## Wat is NetForce?

Wat is NetForce nu eigenlijk? De term NetForce werd voor het eerst geïntroduceerd in een TNO-studie uit 2005.<sup>4</sup> Deze studie behelst een wetenschappelijk benadering van militaire netwerken en introduceert terminologie die is gebaseerd op het concept van *system-of-systems*. Wij zullen die terminologie in dit artikel gedeeltelijk overnemen. NetForce wordt omschreven als het totaal van verbonden knooppunten dat onderling samenwerkt om een specifiek 'netwerk vermogen' mogelijk te maken.

Voor ons doel gaan we NetForce iets specifieker omschrijven, meer toegespitst op de doelstelling van dit artikel. Ten eerste is NetForce een vermogen, een kracht. We omschrijven NetForce hiertoe als het totale



*Principes van NetForce. Bij NetForce zijn ook andere partijen dan Defensie betrokken, waardoor er meer mogelijkheden zijn om effectief te kunnen zijn*

vermogen dat een adaptief militair netwerk kan ontwikkelen (zowel intern als extern de eigen organisatie). NetForce is dus een manier om slagkracht te genereren in brede zin.

In de tweede plaats is NetForce een fysieke verschijningsvorm, waarbij we NetForce omschrijven als een optimaal vertakte militaire geweldsorganisatie, die, om beslissend te kunnen zijn in het gevecht, slim en legitiem gebruik maakt van de kracht van moderne netwerken.

Ten derde is NetForce een metafoor. Een metafoor voor een paradigmaverandering van een hiërarchisch geordende geweldsorganisatie naar een genetwerkte geweldsorganisatie. NetForce is een metafoor voor het geheel van veranderingen dat nodig is om Defensie effectief te maken tegen toekomstige opponenten, gebaseerd op omgevingsveranderingen. Dit artikel beoogt de potentiële voor- en nadelen van NetForce uit te leggen.

## NetForce als antwoord

Tegen genetwerkte tegenstanders is een genetwerkte respons effectiever om drie redenen. Allereerst overstijgt het veiligheids-

<sup>3</sup> Idem.

<sup>4</sup> Keus, H.E., Netforce Principles. *An elementary Foundation of NEC and NCO*, TNO, juni 2005.

probleem waarmee we worden geconfronteerd het eigen departement. Innovatieve tegenstanders passen een veelvoud aan inzetmiddelen toe om hun beoogde doelstellingen te bereiken, op een veelvoud van terreinen of domeinen. Of we dit nu met termen zoals *ambiguous warfare* of *hybrid warfare* moeten aanduiden of niet, het is een feit dat rivalen of opponenten gebruikmaken van middelen en mogelijkheden die buiten het traditionele westerse beeld van oorlogvoering vallen. Daarop heeft de huidige wijze van denken over defensie geen coherent antwoord.

## NetForce is onder meer een paradigmaverandering van een hiërarchisch geordende geweldsorganisatie naar een genetwerkte geweldsorganisatie

Opponenten manoeuvreren en calculeren behendig om een zo gunstig mogelijke uitgangspositie te creëren voor hun eigen belangen, waarbij de verworvenheden en spelregels van open liberale democratieën als Nederland op doeltreffende wijze gebruikt worden als wapens. Gebruik van tijd, ruimte en middelen wijkt hierbij aanzienlijk af van westers politiek-militair denken.<sup>5</sup> Militaire macht wordt bijvoorbeeld omzeild of verlamd door structureel en op grote schaal informatie te manipuleren, zodat een breed publiek wordt beïnvloed.

### Interdepartementale aanpak

Alleen een meervoudige aanpak die alle machtsinstrumenten benut is hiertegen effectief. Dat overschrijdt alle veiligheidsdomeinen. Die aanpak is dus per definitie niet beperkt tot Defensie alléén. Deze meervoudige aanpak moet ook nog eens snel ingezet kunnen worden. Niet alleen reactief, maar liefst ook proactief. Dit vereist dus nieuwe organisatievormen om sneller en adaptiever op te kunnen treden, die schaalbare capaciteiten kunnen genereren.

Omdat interne en externe veiligheid inmiddels verweven zijn en alle aspecten van onze samenleving raken, is een interdepartementale aanpak of *comprehensive approach* niet meer voldoende. De ene keer is een financiële veiligheidsdreiging een aanvalsmethodiek van een tegenstander<sup>6</sup>, de volgende keer is het een destabiliserende dreiging op humanitair gebied. Elk veiligheidsprobleem vergt dus een specifieke combinatie van genetwerkte capaciteiten om te interveniëren. Het kunnen mobiliseren en aanspreken van de benodigde hulptroepen (ook individuen en het bedrijfsleven, een *whole of society*-benadering) is noodzakelijk: elk probleem en gewenst effect heeft andere schaalbare capaciteiten in het netwerk nodig.

Optimaal genetwerkte organisaties, die onbekende capaciteiten snel kunnen opnemen, waarbij informatie onderling snel kan worden uitgewisseld en waarbij besluitvorming is gedelegeerd naar de lagere niveaus, zijn hiertoe in staat. Bij dreigend geweld of grote maatschappelijke ontwrichting, kan Defensie als platform- of parapluorganisatie dit geheel als betrouwbare en legitieme partij orkestreren of stroomlijnen. Hierdoor worden alle initiatieven effectief gericht, ook wanneer er niet altijd sturende controle kan zijn over de uitvoering.

### Uiteenlopende verbanden en verschijningsvormen

Ten tweede nemen interstatelijke conflicten af en werken tegenstanders steeds vaker in uiteenlopende verbanden of (tijdelijke) verschijningsvormen, al dan niet verweven met andere (criminele) netwerken, stamverbanden,

<sup>5</sup> Zie noot 2.

<sup>6</sup> Bijvoorbeeld het devalueren van een munt, of anderszins het op grote schaal ondermijnen van het vertrouwen in een munteenheid, waardoor een maatschappij in elkaar stort.



FOTO: U.S. ARMY, R. SUMMITT

Tegenstanders werken steeds vaker in uiteenlopende verbanden, al dan niet verweven met andere (criminele) netwerken, stamverbanden of ad-hoc-milities

ad-hoc-milities, et cetera. Tegenstanders zijn moeilijk herkenbaar als combattant en bedienen zich van een mengvorm die regelmatig van vorm verandert.

Met andere woorden: opponenten genereren vermogen, kracht en voortzettingsvermogen door zich te vormen als een hybride netwerk. De huidige wijze van het bestrijden van netwerken werkt dan niet meer.<sup>7</sup> Een overgang van een *organisatie-centric approach* naar een *actor-centric approach* is daarom nodig. De beste wijze om een ongewenst, bedreigend (of wijdvertakt) netwerk te bestrijden is om zelf eveneens een netwerk te organiseren. Er komen dan veel meer instrumenten, kennis en kunde ter beschikking dan alleen de 'eigen middelen'.<sup>8</sup> Van het verslaan van vijandelijke formaties naar het verslaan van ongewenste netwerken, vraagt een doctrinaire heroriëntatie.<sup>9</sup>

### Een nieuwe conflictomgeving

In de derde plaats is het noodzakelijk zich te realiseren dat hyperconnectiviteit invloed heeft op tijd- en ruimtifactoren van militaire operaties. Conflicten zijn mondiaal geworden, en amper te beperken in tijd en ruimte. Een *battlespace* is immers niet meer af te bakenen tot alleen een *area of operations*. Een conflictomgeving moet dus, anders als een afgebakend gebied van militair handelen, worden beschouwd als een wereldwijd verbonden veiligheidsecosysteem, ook vanuit militair oogpunt.

7 Traditioneel wordt een *Centre Of Gravity* bepaald, het leiderschap onthoofd en vervolgens verwacht men dan dat het netwerk in elkaar stort, hetgeen bij netwerkorganisaties als al-Qaida, ISIS en Hezbollah niet werkt. Ook innovatieve statelijke actoren blijken zeer levensvatbaar, zoals het regime in Syrië.

8 McChrystal, S.A., <http://foreignpolicy.com/2011/02/21/it-takes-a-network/>.

9 Voelz, G.J., *The Rise of Iwar: Identity, Information, and the Individualization of Modern Warfare*, Strategic Studies Institute en U.S. Army War College Press, 2015.

Het fysieke landschap blijft uiteraard relevant, maar staat niet meer op zichzelf. Juist het menselijke landschap (datgene wat mensen drijft) en het informatielandschap (alle data, informatie en overdracht hiervan, al dan niet gemanipuleerd) vormen alle drie belangrijke

Alleen een meervoudige aanpak die van alle machtsinstrumenten gebruik maakt is effectief. Dat overschrijdt alle veiligheidsdomeinen

terreinen waarop gevochten wordt in moderne operaties. Ze zijn doorslaggevend voor militair succes.<sup>10</sup> Tegenstanders kunnen direct onze maatschappij ontwrichten, ons thuisfront en onze politici beïnvloeden via (social) media, cyberwarfare en allerlei andere instrumenten. Hiermee wordt ook de militaire operatie beïnvloed. Versimpeling van de werkelijkheid helpt niet in een hyperconnectieve wereldorde; het is beter de complexiteit in stand te laten en chirurgisch in te grijpen op essentiële knooppunten.

#### Meer mogelijkheden

NetForce als netwerk leidt ertoe dat er uit meerdere partijen dan alleen Defensie kan worden geput. NetForce biedt dus meer *tools* voor een militaire commandant om zijn opdracht te realiseren. Door kennis, inspanningen en capaciteiten ook van buiten het eigen departement te koppelen en effectief te richten worden veel meer mogelijkheden aangeboden om in alle drie landschappen effectief te kunnen zijn, zelfs wereldwijd.

Een netwerk is immers wijdvertakt en is door die diversiteit in staat om op veel plaatsen tegelijkertijd effecten te genereren. Informatie kan snel binnen het netwerk worden uitgewisseld, aangezien het netwerk immers niet is gekoppeld aan lands- of organisatiegrenzen.

NetForce is daarmee grenzenloos. Het militaire deel van het netwerk moet daarom vertakt zijn binnen de maatschappij, het bedrijfsleven en naadloos zijn aangesloten op het interdepartementale netwerk om overal op de wereld effecten kunnen bewerkstelligen. Partnernetwerken kunnen dan namens de staat mondiaal werkende hybride dreigingen opvangen of voorkomen. Tot dusver is de noodzaak tot verandering, het begrip NetForce en het nut en de noodzaak van genetwerkt militair vermogen toegelicht. Hierna werken we de functies van NetForce en de basisprincipes verder uit aan de hand van onderliggende concepten. Vervolgens komen de sterkten en zwakten hiervan aan bod.

### Netwerkfuncties van NetForce

NetForce kent netwerkfuncties; functies die benodigd zijn om uitvoering te kunnen geven aan het genetwerkte optreden. Deze functies zijn: effecten genereren (*affect*), sturen (*command*), waarnemen (*sense*), beschermen (*shield*), onderling afstemmen (*attune*) en in stand houden (*sustain*).

#### Effecten genereren

*Affect* is de functie die alle activiteiten van het optreden in drie landschappen integreert. Het doel is effecten te genereren om de gewenste invloed te bereiken met het totaal aan beschikbaar vermogen. *Affect* is breder dan alleen slagkracht, manoeuvre en engagement; het omvat het hele spectrum van directe en indirecte, letale en non-letale effectbrengers binnen de drie landschappen.

Al deze effectbrengers dragen bij aan de geïntegreerde boodschap, in lijn met de beoogde doelstelling of opdracht. De verschillende effecten manifesteren zich binnen en buiten de tijdshorizon van de operatie, en met meer of minder controle over de uitkomst.

#### Sturen

*Command* behelst de aansturing van een operatie om de gewenste doelstellingen te realiseren, zodat synergie ontstaat tussen middelen, mogelijkheden (in tijd en ruimte) en

10 Zie hiervoor ook de DOKM studie 'Delphi: Informatie als wapen, middel en doel.'



effect. *Command* richt en verbindt de overige functies in het behalen van een specifiek doel op geïntegreerde wijze.

De functie *command* wordt uitgevoerd binnen de leidende filosofie van opdrachtgerichte commandovoering. Om deze functie tot haar recht te laten komen in dynamische, onzekere en complexe omgevingen, dient de beslissingsbevoegdheid tot op het laagst mogelijke niveau te worden gelegd, waarbij de randvoorwaarden door de orkestrerende lagen worden verzorgd.

Ondanks de toenemende beslissingsondersteunende systemen, doet dit geen afbreuk aan het menselijke karakter van operaties, gebaseerd op vertrouwen, wilsoverdracht en het nemen en geven van verantwoordelijkheid. Omdat afstemming in JIMP-verband<sup>11</sup> de norm is, zal de mate van *control* variëren in het verloop van (delen) van een operatie. In plaats van ‘*span of control*’ spreekt men daarom van ‘*span of influence*’.

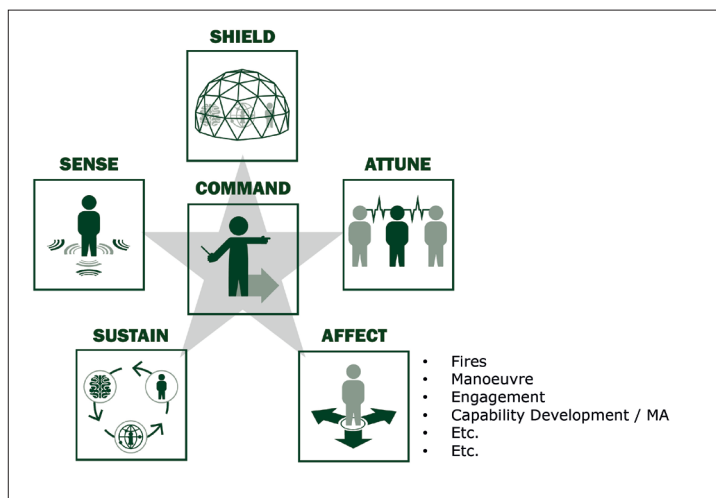
### Waarnemen

De functie *sense* integreert het toenemende geheel aan beschikbare gegevens en informatie in een omvangrijk en toegankelijk systeem, zonder verzuiling per niveau, entiteit, domein, landschap of locatie. Elke sensor, bron, handeling of interactie (*affect*) leidt immers tot gegevens en informatie. Deze leiden, al dan niet gecombineerd, tot een omvattend maar dynamisch omgevingsbeeld.

Uit het geheel van beschikbare gegevens vindt analyse plaats van de relevante informatie om tijdige besluitvorming per niveau, locatie of entiteit mogelijk te maken. Op basis hiervan kunnen kansen en bedreigingen worden geïdentificeerd.

### Beschermen

Het doel van *shield* is het behoud van vrijheid van handelen, zodat een operatie succesvol kan verlopen. De (potentiële) inbreuken op de fysieke, mentale en conceptuele componenten van het beschikbare vermogen worden tegengegaan. *Shield* omvat alle stadia van een



Figuur 3 Samenhangende functies van NetForce optreden

operatie, in de breedste zin, zowel actief als passief, en is niet beperkt in tijd, locatie of landschap.

Risicoafwegingen zijn nodig, omdat het welslagen van een operatie voorop staat en een te strikte afscherming het benutten van kansen, adaptiviteit, samenwerking met anderen of de taakuitvoering in de weg kan staan. Het toenemende aantal factoren van invloed op een operatie brengt met zich mee dat er ook steeds meer indirecte kwetsbaarheden kunnen ontstaan.

### Onderling afstemmen

*Attune* omvat alle interne en externe afstemmingsinspanningen om het geheel aan beschikbaar vermogen effectief te kunnen genereren. Hedendaags optreden is niet langer homogeen maar *joint*, *interagency*, *multinationaal*, lokaal of met een diversiteit aan publieke organisaties (JIMP) op alle niveaus. In iedere operatie wordt, doorgaans in snel wisselende samenstellingen, intensief samengewerkt in elke organisatielaag, met personen of partijen die uit een andere cultuur komen en een diversiteit aan achtergronden en denkbeelden met zich meebrengen.

11 JIMP is de doctrinaire afkorting voor het geheel van *Joint, Interagency, Multinational, Public organizations*.



FOTO: MCD, K. DOGER

*Dankzij de revolutie in informatietechnologie beschikken vectoren op uitvoerend niveau over voldoende omgevingskennis ('situational awareness') of zelfs omgevingsbegrip ('situational understanding')*

Wederzijds begrip, wederzijds vertrouwen en het hanteren van een eenduidige doelstelling blijft echter essentieel voor een effectieve taakuitvoering. Ad-hoc-inzet met partners als norm gaat niet altijd vanzelf. Werken in bijvoorbeeld samengestelde multinationale eenheden en werken met andere overheidsinstanties, optreden in een andere cultuur of met andere culturen vereist continu aanpassing. Verwaarlozing van de functie 'afstemming' leidt daarbij onmiddellijk tot verminderd wederzijds begrip en daardoor verminderde effectiviteit.

#### **In stand houden**

*Sustain* integreert alle inspanningen die nodig zijn om de conceptuele, mentale en fysieke component op te bouwen en in stand te houden. Deze functie omvat het totaal aan inspanningen om een operatie te kunnen handhaven en voort te zetten, totdat de doelstelling of opdracht is behaald, ongeacht

tijd, ruimte of landschap. In de volgende alinea's gaan we een stapje verder en nemen we een voorschot op de componenten waaruit een NetForce zou kunnen bestaan en hoe deze zouden kunnen opereren. We introduceren de basis (netwerk-)elementen van NetForce. Vervolgens leggen we uit hoe we met deze basiselementen willen optreden.

### **Basisgedachte en optreden NetForce**

NetForce bestaat niet uit de traditionele militaire hiërarchische structuur van groep tot legerkorps. Sterker nog, de organisatievorm van NetForce is zo 'plat' als mogelijk. Natuurlijk zijn er wel besluitvormende en ondersteunende elementen nodig, de nadruk ligt evenwel op het zelf kunnen synchroniseren van uitvoeringselementen. We noemen deze individuele uitvoerende basiselementen vectoren.<sup>12</sup>

## Vectoren

Een vector is een handelend element, en kan taken of activiteiten uitvoeren. De omvang van een vector is niet vooraf gedefinieerd en de functie hangt af van het kennisniveau, de conflictomgeving, het op te lossen probleem en de bijbehorende dynamiek. De bindende factor tussen de vectoren is uiteraard een gezamenlijke doelstelling, evenals de *drive* om specifieke taken uit te willen voeren. Om deze reden kunnen ook vectoren zonder structurele bevelsrelatie deel uitmaken van NetForce. Het gaat om de bereidheid tot het genereren van effecten; de organisatie staat niet meer centraal.

De revolutie in informatietechnologie maakt het immers mogelijk dat vectoren op uitvoerend niveau over voldoende omgevingskennis of zelfs omgevingsbegrip beschikken en dat zij hun eigen rol het beste kunnen inschatten op basis van hun identiteit en taakvolwassenheid. Ze zijn dus zelfsynchrooniserend. Door onderlinge synchronisatie ontstaat niet alleen *situational awareness* maar ook *situational understanding*.

Het optreden van vectoren in het netwerk is vooral gebaseerd op de *power-the-edge* gedachte.<sup>13</sup> Alle vectoren voeren daarmee zelf, in meer of mindere mate, de netwerkfuncties uit. Zo hebben ze een eigen besluitvormende functie (*command*), verzamelen en delen omgevingsinformatie (*sense*), stemmen af (*attune*), genereren effecten (*affect*) en hebben zoveel mogelijk een eigen beschermings- en voortzettingstaak (*shield* en *sustain*).

Voor de krijgsmacht geldt dat vectoren, net als conventionele eenheden, moeten worden opgeleid en genormeerd, ook vanwege de cohesie, het onderlinge vertrouwen en het kunnen afleggen van verantwoording. De vectoren, 'legoblokjes' hebben om deze praktische reden initieel een vaste samenstelling als basis. Deze kern kan vervolgens wisselen bij inzet, naar gelang de benodigde dichtheid of schaalgrootte.

## Hubs en nodes

Om het zelfstandige optreden van de vectoren te optimaliseren kunnen de vectoren worden

ondersteund door hubs. Een hub is een aansluitpunt op een netwerk, waardoor data, diensten of goederen kunnen worden uitgewisseld tussen meerdere vectoren of tussen groepen van vectoren.

Voor het besluitvormend element waar koers en richting wordt bepaald voor (delen) van het netwerk wordt de term *node* gebruikt. Een

Bij NetForce gaat het om de bereidheid tot het genereren van effecten; de organisatie staat niet meer centraal

*node* is een knooppunt waar meerdere stakeholders binnen het veiligheidsecosysteem gezamenlijk afspraken maken over de koers en richting, of voorzien in elkaars netwerkfuncties als dit opportuun is. Nodes zorgen daar waar nodig voor sturing (*command*), eventueel randvoorwaarden en zijn concentraties van dataverkeer. Nodes kunnen het plannen en uitvoeren van een reeks van activiteiten autoriseren en hebben dus ook een voorwaardenscheppende functie.

Op basis van netwerkopdrachten en zelf-synchronisatie stemmen de diverse vectoren hun activiteiten zoveel mogelijk zelf af. Ze hoeven dus geen toestemming te vragen voor actie. NetForce streeft naar een zo hoog mogelijk niveau van autonome actie door de netwerkelementen, waarbij tegelijkertijd het vermogen tot massale effecten in stand worden gehouden. Dit gebeurt door onderlinge of gecoördineerde synchronisatie, waarbij de effecten uit meerdere fysieke 'richtingen' of 'invalshoeken' komen zodat de opponent uit

<sup>12</sup> Zie noot 9.

<sup>13</sup> Idem.

evenwicht wordt gebracht (*swarming*). Dat dit prima werkt, bewijzen moderne games, waar taakvolwassen individuen, die allemaal hetzelfde operationele beeld hebben, zeer effectieve teams kunnen vormen zonder elkaar ooit fysiek gezien te hoeven hebben.

## Gezamenlijk optreden

Een toekomstig militair netwerk is dus opgebouwd uit meerdere vormen van vectoren, hubs en nodes. Alle drie elementen zijn nodig voor een effectief netwerk, inclusief de onderlinge verbindingen. Vectoren alléén vormen geen netwerk. Ook is een militair netwerk niet vooraf vast gedefinieerd, zoals dat nu vast geklonken wordt in organogrammen. Naar gelang het campagnethema, de intensiteit ervan en de te bereiken (politieke, militair-strategische) doelstelling kan elke keer een op maat gesneden militair netwerk worden opgebouwd.



Een toekomstig militair netwerk is opgebouwd uit meerdere vormen van vectoren, hubs en nodes

Bovendien kan het, indien noodzakelijk, gebouwd, aangevuld en/of aangepast worden met civiele, positionele en inheemse elementen. Ook is het mogelijk om tussentijds aanpassingen van het netwerk door te voeren. Alle netwerkelementen moeten wel *compatible* zijn met het netwerk en het vermogen hebben in korte tijd af te stemmen (*attune*) met onbekende partners.

Interoperabiliteitsprotocollen zijn dus nodig, evenals het trainen van het vermogen om af te stemmen. Daarnaast is het belangrijk dat andere netwerkelementen bewust gemaakt moeten worden dat er nieuwe netwerkelementen aan het netwerk deelnemen. Anders kunnen ze immers niet van elkaars toegevoegde waarde gebruik maken. Ook statusveranderingen van de netwerkelementen moeten aan elkaar worden doorgegeven. Dit betekent ook: onderzoeken hoe de waarde van bestaande militaire grondbeginselen zich verhouden in een dergelijk systeem. Beginselen als eenhoofdige leiding, verantwoording kunnen afleggen en niveaus van verbijzondering van informatie zijn zo waardevol dat ze mogelijk in een andere vorm ook in nieuwe militaire inzetvormen ingebracht moeten worden.<sup>14</sup>

## Manoeuvre

Vectoren treden vrijwel altijd verspreid op. Daar waar in vroegere tijden militaire eenheden (in de breedte of diepte) gegroepeerd moesten worden om hun vuurkracht te optimaliseren met behulp van de destijds beperkte *Command & Control* (C2) methodes, is dat nu niet meer nodig. Omdat zowel de vuurkracht van de individuele vectoren is toegenomen en de C2-techniek een grotere *span of control* toelaat, is het niet meer nodig eenheden dicht bij elkaar te groeperen.

Vectoren kunnen nu over grotere ruimtes worden verspreid met behoud van collectieve effectiviteit. Dit heeft twee belangrijke voordelen. Allereerst kunnen eenheden nu vanuit meerdere richtingen opponenten naderen, zodat deze tegelijkertijd voor meerdere

14 Zie noot 4, pagina 8.



FOTO: MCD, E. KLJIN

Een netwerk kan zich verdichten om een grotere macht op te vangen of uitdijen om een groter bereik te hebben. Een militaire netwerk kan dus zowel massa opvangen als massa(le) effecten genereren

uitdagingen wordt gesteld (*swarming*). Hierdoor wordt de tegenstander psychologisch en fysiek uitgemanoeuvreed. Ten tweede kunnen we door de verspreiding de eigen beweeglijkheid optimaal uitbuiten en daarmee de eigen kwetsbaarheid verminderen. Het militaire netwerk wordt daarmee ongrijpbaar. Deze manier van optreden noemen we *Advanced Dispersed Operations* (ADO).

Vectoren zijn optimaal beweeglijk en hebben het vermogen in en uit de conflictomgeving te bewegen. Bijvoorbeeld naar een veiligere omgeving om te rusten of te recupereren. Ook kunnen ze naar behoefte concentreren of verspreiden. ADO sluit zelfs niet uit dat er lineair opgetreden kan worden. Ook dit behoort nog altijd tot de mogelijkheden, maar vraagt wel oefening. Bovendien kost het tijd om de

vectoren lineair te arrangeren en neemt de kwetsbaarheid van de eigen vectoren hierdoor toe. Ze worden 'identificeerbaarder' en minder beweeglijk, dus kwetsbaarder. Naast 'swarming' en 'ADO' is het NetForce gedachtegoed gebaseerd op een groot aantal internationaal erkende concepten.<sup>15</sup>

15 De hier gepresenteerde ideeën zijn gestoeld op meerdere concepten. NetForce leiderschap bouwt voort op het concept '*Distanced an distributed leadership*'. NetForce manoeuvre is gebaseerd op het concept '*swarming*' en '*advanced dispersed operations*'. NetForce *attune* is een uitwerking van de concepten '*virtual collaboration*' en '*loose coupling*'. NetForce *sustain* bouwt voort op de concepten '*self-reliant units*' en '*hub-and-spoke network*'. De NetForce organisatie is een operationalisatie van de concepten '*pools of capacities*' en '*facilitating network*'. NetForce *command* operationaliseert de concepten '*reach back*', '*mission command*', '*reverse accountability*', '*broad distribution of information*', '*distributed decision-making*' en '*pooling information*'.



FOTO MCD. J. VAN HEUVER

*De introductie van de computer en internet heeft geleid tot een 'informatierevolutie'. De vraag is nu wat er precies gaat veranderen aan het militair vermogen in het informatietijdperk*

Het is belangrijk om zich te realiseren dat NetForce een geweldsmonopolie faciliteert. NetForce kan dus beschadigen, vernietigen, verwonden en doden. Zonder het bezit van dergelijke fysieke krachten is elke dreiging met de inzet van geweld immers ongeloofwaardig en verliest elke toekomstige militaire organisatie haar relevantie. NetForce is dus ultimo een genetwerkte geweldsorganisatie, die actoren in haar omgeving kan dwingen hun gedrag te veranderen.

### **Sterke punten van NetForce**

Een netwerk als organisatie vorm kent voor- en nadelen. Allereerst de voordelen. Ten eerste heeft een netwerk een sterk absorptievermogen. Het vernietigen van een paar verbindingen

heeft geen grote invloed op de sterkte van het netwerk. Ten tweede kan een netwerk van 'dichtheid' (de zogeheten entropie) veranderen zonder samenhang te verliezen. Het kan zich verdichten om een grotere macht op te vangen of uitdijen om een groter bereik te hebben. Een militair netwerk kan dus zowel massa opvangen als massa(le) effecten genereren.

In de derde plaats kan een netwerk overal effect genereren. Met andere woorden: het is niet gebonden aan een domein, niet beperkt in tijd of ruimte, en is in meerdere conflictvormen bruikbaar. Ten vierde kan een netwerk van vorm veranderen. Dit betekent dat een militaire verschijningsvorm aangepast kan worden met politionele, civiele of inheemse uitbreidingen.

Het vijfde voordeel is dat een netwerk relatief ongrijpbaar is. Het kent immers nauwelijks fysieke aangrijpingspunten en kan zichzelf bovendien snel herstellen doordat netwerkelementen in staat zijn zelfstandig verbindingen naar elkaar op te bouwen of te herstellen. Het zesde kenmerk is beweeglijkheid. Een netwerk kan ook bij grote dynamieken zijn onderlinge samenhang behouden. En juist die beweeglijkheid (zowel in fysieke als conceptuele zin) biedt tegenover hybride dreigingen grote voordelen, omdat de eigen kwetsbaarheid minder is.

Het zevende kenmerk is diversiteit. Een netwerk heeft meer mogelijkheden (zoals uitbreiding en schaalbaarheid) en reikwijdte (organisatie overstijgend) dan een hiërarchische organisatie met een vastgelegde organisatie-tabel. Hierdoor kan ook veel sneller een beroep gedaan worden op kwaliteiten die niet voorheen voorhanden of voorzien waren. Als laatste kent een netwerk niet alleen een fysieke verschijningsvorm, maar ook een virtuele verschijningsvorm. Elementen kunnen onderling gecoördineerd optreden, zonder fysieke verbindingen te hebben. Een netwerk is feitelijk één van de meest adaptieve verschijningsvormen, eindeloos aanpasbaar en eindeloos uit te breiden.

### Zwakke punten van NetForce

Een netwerk kent natuurlijk ook zwakten.<sup>16</sup> Ten eerste is belangrijk om te beseffen dat bij een netwerk de onderlinge verbindingen de kracht betekenen, niet de afzonderlijke netwerkelementen. Als deze verbindingen relatief zwak zijn, is het gehele netwerk zwak. Niet-geïnterrumpeerde verbindingen zijn daarmee een absolute voorwaarde voor kennisdeling. Het aantal kanalen, middelen, mogelijkheden en modaliteiten waarmee gecommuniceerd kan worden, is de afgelopen decennia echter exponentieel gegroeid en zal naar verwachting alleen maar toenemen, zodat meervoudige redundantie dit grotendeels kan omzeilen.

Ten tweede moeten netwerkelementen bereid zijn om voor een gezamenlijke idee te vechten,

maar ook met en voor elkaar. Vertrouwen en cohesie, het opbouwen van gelijke normen en waarden, zijn lastig te genereren in snel op- en afbouwende netwerken, tenzij hier al een basis voor ligt, bijvoorbeeld het hebben van een gezamenlijke cultuur of identiteit. Het gezamenlijk belang moet dus groter zijn dan het individuele belang. Schaalgrootte van het netwerk lost dit probleem deels op; er zijn immers altijd mensen bereid zich in te spannen en een bijdrage te leveren, en deze kunnen via velerlei kanalen gemobiliseerd worden.<sup>17</sup>

Juist de beweeglijkheid van een netwerk (zowel in fysieke als conceptuele zin) biedt tegenover hybride dreigingen grote voordelen, omdat de eigen kwetsbaarheid minder is

Critici uiten de zorg dat NetForce niet in staat zou zijn om een conventioneel optredende strijdmacht te verslaan, omdat fysieke massa ontbreekt. Massa, dat wil zeggen numeriek overwicht, blijft wel degelijk een factor van belang. Het samenbrengen van massa is bij een netwerk weliswaar mogelijk, maar kost meer tijd dan bij een hiërarchisch georganiseerde krijgsmacht.

Hier valt tegenin te brengen dat het bij militair optreden niet gaat om fysieke massa (die is immers tijdelijk), maar vooral om kritische massa (genoeg mensen die aanhanger zijn van het idee) en massa van effecten. En het

16 Een interessante argumentatie tegen militaire netwerken geven R.E. Griffin en D. J. Reid in hun thesis: *A Woven web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy*, gepresenteerd op het achtste International Command and Control Research & Technology Symposium, juni 2003.

17 Jihadistische strijdgroepen als al-Qaida en ISIS tonen dit effectief aan.

aanbrengen van massale effecten is bij een genetwerkte organisatie eenvoudiger dan bij een hiërarchische krijgsmacht. Bij een netwerk kunnen immers effecten vanuit het gehele netwerk worden opgeroepen, terwijl dit bij een hiërarchische krijgsmacht alleen vanuit de bovenliggende bevelslagen mogelijk is.

## Afsluiting

U heeft dit bovenstaande wellicht gelezen en hier voor uzelf kanttekeningen bij geplaatst, al dan niet vol ergernis, enthousiasme of verwondering. Mooi! Hierbij doen we een beroep op u om met ons mee te denken. Voor het onder-

Het zal inmiddels duidelijk zijn dat wij openstaan voor een discussie over andere vormen van militair vermogen, om in lijn met de technologische en omgevingsveranderingen en het optreden van tegenstanders ook in de toekomst relevant en succesvol te kunnen blijven. De complexiteit van dreigingen om ons heen, de houdbaarheid en betaalbaarheid van het huidige model en het optreden van tegenstanders moeten naast professionalisme, voldoende *sense of urgency* bieden om andere mogelijkheden te willen onderzoeken en hier niet de ogen voor te sluiten.

In dit artikel hebben we een eerste zienswijze geschetst van de manier waarop een dergelijk netwerk kan worden gevormd en kan optreden. Nader wetenschappelijk onderzoek en militaire experimenten zijn noodzakelijk om het NetForce gedachtegoed te verbeteren.

De uitdaging is om ruimte te geven aan het ontwikkelen van innovatieve ideeën en ervoor te zorgen dat zij niet ten onder gaan aan controlemechanismen. We vragen daarom twee dingen. Ten eerste doen we een beroep op alle ‘verandergeesten’ binnen Defensie om de NetForce gedachte te omarmen, mee te helpen ontwikkelen, verder te volmaken, problemen helpen op te lossen en NetForce tijdig naar volwassenheid en toepasbaarheid te stuwen.

In de tweede plaats vragen we de meer ‘behoudende krachten’ binnen Defensie om NetForce een kans te geven en een gezond tegenwicht te bieden. Door tegenwicht kan de kennis over NetForce worden uitgedaagd, verdiept en verbreed. Door NetForce grondig te onderzoeken, te beproeven, te testen, ervaringslessen vast te leggen en verbeteringen door te voeren kan Defensie klaar gemaakt worden voor de toekomst.

Effectief gebruikmaken van de omgeving en anticiperen op tijdperkveranderingen is in onze ogen dé manier om te zorgen dat het Nederlandse militaire vermogen klaar is voor conflicten van de toekomst. ■

Er zijn naast *command* nog voldoende vragen te beantwoorden rond schaalbaarheid, vertrouwen en cohesie, voortzettingsvermogen, grondbeginselen en de overige netwerkfuncties

zoeken van alle aspecten en de haalbaarheid van NetForce is sinds januari 2016 namelijk een onderzoek opgestart door TNO in samenwerking met de krijgsmacht. Dit TNO-onderzoek (V1604), begeleid door het Land Warfare Centre, richt zich in het eerste onderzoeksjaar op de concepten die deel uitmaken van een militaire genetwerkte eenheid.

Vanaf het tweede jaar ligt de nadruk op de netwerkfunctie *command*, omdat dit de essentiële verbindende functie van militair optreden is die fundamenteel verandert in de NetForce wijze van optreden. U kunt hiervoor contact opnemen via [lwc@mindef.nl](mailto:lwc@mindef.nl) of met een van de auteurs. Er zijn immers naast *command* nog voldoende vragen te beantwoorden rond schaalbaarheid, vertrouwen en cohesie, voortzettingsvermogen, grondbeginselen en de overige netwerkfuncties.