Jaargang 182 nummer 9 - 2013

MILITAIRE SPECTATOR

Cyber-operaties en militair vermogen

- Storytelling: a lifesaving tool?
- Het begin van eeuwige oorlog

MEDEDELING

Vereniging Informatici Defensie

René Olthuisprijs 2013

Eén van de doelstellingen van de Vereniging Informatici Defensie (VID) is het bevorderen van de deskundigheid op het gebied van informatica. De vereniging doet dat onder meer door het jaarlijks toekennen van de René Olthuis scriptieprijs. Het gaat om een aanmoedigingsprijs voor een scriptie, publicatie of artikel over het vakgebied IV of ICT. Het onderwerp is – bij voorkeur – een actueel (Defensie)vraagstuk binnen de IV of ICT. De prijs bestaat uit een geldbedrag van 250 euro en een bijbehorende herinnering.

De VID heeft een reglement opgesteld met de voorwaarden waaraan een scriptie, publicatie of artikel moet voldoen. Het reglement is te downloaden van de intranetsite van de VID (http://intranet.mindef.nl/portaal/service/verenigingen/vid/index.aspx) of op te vragen bij de secretaris van de VID (Secretaris.VID@mindef.nl). Inzendingen kunnen naar het e-mailadres van de secretaris worden gestuurd of eventueel per post naar VID, t.a.v. Commissie René Olthuisprijs, Doddendaal 17, 6715 JV Ede.

De sluitingsdatum voor aanlevering is 1 november 2013.

Rectificatie

In het artikel van dr. E. Broos en M. Sissingh MSc. 'Verhelderen van de informatieomgeving voor Information Operations door Systemic Analysis', verschenen in MS 7/8 (2013), is figuur 3 onjuist weergegeven. Een pdf met de correcte figuur – een wiskundig model, ontworpen door de auteurs – is op verzoek bij de bureauredactie te verkrijgen.

in memoriam

Op 11 juli 2013 is op de leeftijd van 65 jaar overleden de oud-redacteur kolonel KLu b.d. dr. Jan van Angeren. Hij was redacteur van de Militaire Spectator tussen 1989 en 1993 en van 2001 tot 2004. Wij herinneren ons Jan als een gedreven redacteur met een grote liefde voor de krijgswetenschappen. Hij ruste in vrede.

De hoofdredacteur

KVBK
KONINKLIJKE VERENIGING TER BEOEFENING VAN DE KRIJGSWETENSCHAP

UITGAVE
Koninklijke Vereniging ter Beoefening van de Krijgswetenschap
www.kvbk.nl
info@kvbk.nl
www.facebook.com/kvbknederland
twitter: @kvbk1

Secretaris en ledenadministratie
Majoor Daan Storm van Leeuwen
DM.StormVanLeeuwen@mindef.nl

Nederlandse Defensieacademie (NLDA)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
ledenadministratie@kvbk.nl

De Militaire Spectator wordt ook verstuurd op basis van rang/schaal. Adreswijzigingen doorgeven bij de eigen personeelsdienst.

De Militaire Spectator is aangesloten bij de European Military Press Association

LIDMAATSCHAP
binnenland € 25,00
studenten € 17,50
buitenland € 30,00

OPMAAK EN DRUK
Drukkerij Ten Brink
ISSN 0026-3869

Coverfoto:
Foto Reuters, K. Pempel

MILITAIRE SPECTATOR

Vertrouwen

Kranten melden dat het vertrouwen van het eigen personeel in Defensie daalt. Volgens *Trouw* kraakt het binnen de krijgsmacht, is het personeel onzeker en maakt de leiding zich hier ernstige zorgen over.[1] Aanleiding voor deze berichtgeving is een intern onderzoek van het Dienstencentrum Gedragswetenschappen, waaruit blijkt dat het vertrouwen in Defensie als werkgever veel lager is dan enkele jaren geleden.
In het editoriaal in de *Militaire Spectator* van juli/augustus is al aangegeven dat een opeenstapeling van reorganisaties en onzekerheid over de toekomst de balans voor het defensiepersoneel mogelijk negatief doet doorslaan en het werken bij Defensie niet meer aan de verwachtingen voldoet.[2]

Het is zaak dat de politiek helderheid verschaft over de aard en de omvang van de krijgsmacht

Vertrouwen heeft in zowel sociale als psychologische zin meerdere betekenissen.
De meest gangbare definitie van vertrouwen omvat doorgaans de volgende elementen: de bereidheid van een persoon of groep om afhankelijk te zijn van de daden van een andere persoon of groep, geloven dat een ander eerlijk is of dat iets goed zal gaan en de verwachting van een persoon dat degene die hij/zij vertrouwt zal handelen op een manier die hem/haar niet zal benadelen, met het risico in een nadelige positie te belanden als de ander dit vertrouwen schaadt.[3] Alle drie de elementen lijken bij het gros van het defensiepersoneel de laatste jaren negatief te zijn beïnvloed.
Niet alleen het recente onderzoek, maar ook de (vak)bonden, commandanten en de Inspecteur-Generaal der Krijgsmacht (IGK) hebben dit pijnlijk aan de kaak gesteld.

Opmerkelijk is overigens dat het afgenomen vertrouwen volgens het interne onderzoek niet zozeer ontstaat bij de relaties met collega's en direct leidinggevenden, maar dat de pijn vooral zit bij de wijze waarop de politiek met Defensie omgaat. Met name de bezuiniging van 1 miljard (2012), waardoor 12.000 arbeidsplaatsen verdwijnen, de extra bezuiniging van 333 miljoen (2013) en de zorg om mogelijk nog meer bezuinigingen zijn hier debet aan.

Onduidelijkheid over de logische samenhang van deze bezuinigingen en reorganisaties zou het personeel onrustig maken en het vertrouwen ondermijnen. Maar ook onbegrip over de zwalkende koers die Defensie vaart en het uitstellen en vooruitschuiven van belangrijke besluiten voor de toekomst werken onrust en afnemend vertrouwen in de hand.
In een organisatie waar het personeel gewend is om te handelen naar het oogmerk van de commandant moet er immers wel een (politiek) oogmerk zijn of op zijn minst een stip aan de horizon.

1 'Vertrouwen in Defensie slinkt', *Trouw*, 8 augustus 2013.
2 'Balans!', editoriaal in: *Militaire Spectator* 182 (2013) (7/8) 322-323.
3 Zie: R.C. Mayer, J.H. Davis en F.D. Schoorman, 'An integrative model of organizational trust' in: *The Academy of Management Review*, Vol. 20, No. 3 (juli 1995) 709-734.

Het is dan ook zaak dat de politiek helderheid verschaft over de aard en de omvang van de krijgsmacht. Na ruim twintig jaar snijden zit er volgens ingewijden geen vlees meer op de botten en is de bodem bereikt. Ruimte voor uitbreiding of extra geld om noodzakelijke vernieuwingen bij Defensie door te voeren lijken moeilijk inpasbaar, zo niet onrealistisch, gelet op het begrotingstekort en andere politieke prioriteiten als de zorg, onderwijs en duurzaamheid.

Verder 'kaasschaven' kan – en is wellicht weer politiek opportuun – maar gaat ten koste van bondgenootschappelijke bijdragen, het internationale aanzien en bovenal van het vertrouwen van het huidige en toekomstige personeel. De hoop van velen die de krijgsmacht een warm hart toedragen en de neerwaartse spiraal wensen te doorbreken is dan ook nadrukkelijk gevestigd op de visie van de minister(s) op Defensie.

Dat hier een goede analyse van de omgeving aan voorafgaat is evident en niet zo moeilijk. Belangrijke bouwstenen als de *Strategische Verkenningen* en rapporten van Clingendael en het The Hague Centre for Strategic Studies (HCSS) zijn al door diverse deskundigen aangedragen en wijzen erop dat de wereld er niet veiliger op wordt. Het gaat echter vooral om de keuzes die de politiek en dit kabinet maken om de (internationale) veiligheid en belangen ook te kunnen blijven beschermen met het defensieapparaat. Deze keuzes moeten uiteraard (financieel) uitvoerbaar zijn, een visie uitstralen en een richtpunt vormen voor de koers van de Nederlandse krijgsmacht.

Met een dergelijk afgewogen totaalpakket is vervolgens de ambtelijke en militaire leiding aan zet om de organisatie (opnieuw) te richten en te sturen. Het is immers te gemakkelijk om alles op de politiek af te schuiven. Ook de defensietop heeft een belangrijke taak en rol, met name op het gebied van motivatie en moreel.

De keuzes moeten uitvoerbaar zijn, een visie uitstralen en een richtpunt vormen voor de koers van de Nederlandse krijgsmacht

De vraag naar zicht op toekomstperspectief en invulling van de rol als aantrekkelijk werkgever is groot. Het behoud van talent, de ambassadeursrol van het eigen personeel en de wervingskracht om de defensieorganisatie te (blijven) vullen vormen belangrijke aandachtspunten. Het vraagstuk hoe militairen en burgers passen binnen de aangereikte (politieke) visie en missiedoelstellingen zal zodanig uitgewerkt moeten worden dat het de huidige (en toekomstige) werknemers duidelijkheid, perspectief en hoop biedt. Zo kan er bij het personeel van Defensie weer vertrouwen groeien. ■

Cyber-operaties en militair vermogen

Nederland lijkt in toenemende mate het slachtoffer te zijn van cyber-aanvallen. Dat wil zeggen: van cyber-criminaliteit, -spionage en -(h)ac(k)tivisme. Deze 'aanvallen' op DigiD, ING of iDeal waren niet de dreigingen die de minister van Defensie in juni 2012 voor ogen had toen hij de Defensie Cyber Strategie (DCS) lanceerde. Hierin was de ontwikkeling van militair vermogen om cyber-operaties uit te voeren een speerpunt. Tot nu toe is wereldwijd slechts mondjesmaat gebruik gemaakt van cyber-operaties tijdens militaire operaties.[1] Vaak verwijst men hierbij naar *Stuxnet*,[2] maar dit betreft 'cyber-sabotage' oftewel 'cybotage'.[3] Bij de Israëlische operatie *Orchard* zijn cyber-capaciteiten echter wel daadwerkelijk ingezet.[4] Het debat over de vraag hoe de Nederlandse krijgsmacht met dit 'nieuwe' domein zal omgaan is in volle gang.

*Kolonel dr. P.A.L. Ducheine en mr. J. van Haaster, tweede luitenant**

De uitdaging voor Nederland en Defensie is hoe *cyber warfare* in het militaire en veiligheidsdomein moet worden geïncorporeerd. Niet alleen bestaat er discussie of en in welke mate de overheid *cyber security* (meer) tot haar taken moet rekenen,[5] maar ook *hoe* de regering daartoe wordt uitgerust (door de wetgever).

Doel artikel

De vraag 'hoe organiseert de overheid digitale veiligheid (*cyber security*)?' keert ook terug binnen de verantwoordelijkheid van de Commandant der Strijdkrachten (CDS). Een aantal taken in het digitale domein wordt immers bij hem belegd.[6] Het onder de CDS ressorterende Defensie Cyber Commando zal uiteindelijk *cyber*-capaciteiten om moeten zetten in *operationele* capaciteiten die in normale militaire operaties te integreren zijn.[7]

Bij de lancering van de DCS zei de minister van Defensie hierover: 'Ons uitgangspunt is dat de cyber-capaciteiten van Defensie volledig geïntegreerd moeten worden in ons militair optreden'.[8] Met andere woorden, de CDS zal met cyber-capaciteiten bijdragen aan het militaire vermogen van Nederland.

* Kol Ducheine is universitair hoofddocent Cyber Operations aan de NLDA. Tlnt Van Haaster sloot zijn bachelor krijgswetenschappen af met een thesis over *Social Media* (bekroond door VID). De auteurs danken bgen b.d. prof. Hans Bosch, kolonel ir. Hans Folmer, de luitenant-kolonels Edwin de Ronde, mr. drs. Peter Pijpers en Marco Verhagen EMSD en majoor drs. George Dimitriu voor hun suggesties en commentaar.

1 P. Ducheine, F. Osinga & J. Soeters, *Cyber Warfare – Critical Perspectives* (Den Haag, TMC Asser Press, 2012).

2 Stuxnet is software die is aangetroffen in onderdelen van het Iraanse nucleaire programma en die onder meer centrifuges voor de verrijking van uranium ontregelde.

3 Een samentrekking van cyber en sabotage: Albert Benschop, *Cyberoorlog - Slagveld Internet* (Tilburg, Uitgeverij de Wereld, 2013).

4 Zie verder: P. Cornish, D. Livingstone, D. Clemente & C. Yorke, *On Cyber Warfare* (London, Chatham House, 2010).

5 R. Prins, 'Een cyberleger vergt geld en lef', *de Volkskrant*, 4 augustus 2012.

6 Defensie Cyber Strategie 2012 (hierna: DCS). Het Defensie Cyber Commando wordt via single service management bij het Commando Landstrijdkrachten ondergebracht.

7 A. Schnitger & J. Folmer, 'Cyber ontwikkelingen bij Defensie', in: *Intercom* (2012) (4) 17-19. Zie ook DCS.

8 Lezing minister van Defensie Defensie Cyber Symposium 2012 (Breda, 25-6-2012), via: <www.defensie.nl/actueel/nieuws/2012/06/27/46197032/Minister_Hillen_presenteert_Defensie_Cyber_Strategie>.

Hoe de krijgsmacht (en de CDS) cyber-capaciteiten operationaliseert en integreert in het militaire vermogen, is een actuele vraag die ook in de *Militaire Spectator* aandacht krijgt.[9] Ons doel is bij te dragen aan de conceptuele vraag welke plaats cyber-operaties innemen binnen 'militair vermogen' en hoe de krijgsmacht *cyber warfare* kan operationaliseren.

In het bijzonder stellen we ons de vraag waartegen cyber-operaties zich richten (adressaat of aangrijpingspunt) en welke effecten met cyber-middelen kunnen worden bereikt.

Opzet

We zullen in deze bijdrage de conceptuele en doctrinaire vragen binnen het militaire machtsinstrument aan de orde stellen. Daarbij concentreren we ons op de eerste en de tweede hoofdtaak: verdediging, en handhaving en bevordering van de internationale rechtsorde. Om niet alleen maar ingewijden in de militaire doctrine te bereiken bezien we eerst de essentiële aspecten van de gangbare conceptuele en doctrinaire benadering van reguliere militaire operaties.[10] Daarna bespreken we 'militair vermogen' en haar context, alsmede de inzet van militair vermogen, oftewel operaties. We staan stil bij de vraag welke effecten met operaties worden beoogd, welke middelen en methoden daarvoor bestaan en waartegen ze zich richten.

Onze hoofdinspanning betreft de introductie van het digitale domein in het militair vermogen. We beschrijven de bijzondere en gelaagde structuur van *cyberspace* en bepalen de cyber-elementen binnen de drie componenten van militair vermogen.

Vervolgens definiëren en beschrijven we cyber-operaties, en kijken we waar deze operaties zich op richten, welke effecten mogelijk zijn en welke middelen en methoden daarbij gebruikt zouden kunnen worden.

Uitgangspunten, definitie & beperkingen

Om een eenduidige begripsvorming te realiseren baseren we ons allereerst op gangbare begrippen uit de militaire doctrine.[11] We beschrijven de generieke doctrine overigens slechts op hoofdlijnen. Daarnaast hanteren we een internationaal gangbare definitie voor militaire cyber-operaties:[12]

> *The employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace*.[13]

Het uitvoeren van cyber-operaties hebben we hiervoor aangeduid als *cyber warfare*.[14] Wat *cyber capabilities* zijn, welke doelstellingen te realiseren zijn en waaruit cyberspace bestaat, zullen we later in meer detail uiteenzetten.[15]

Van militair vermogen naar operaties

Veiligheid garanderen is een van de kerntaken van de staat. Voor de realisatie van veiligheidsbeleid en (andere) strategische doelen beschikken staten over meerdere machtsmiddelen: diplomatieke, economische, militaire en informatie.[16] Het doel van de inzet van deze machtsmiddelen is het beïnvloeden van (het gedrag van) andere actoren waardoor veiligheidsbeleid en strategische doelen te realiseren zijn. 'De Nederlandse defensie-inspanning is gericht op het nationaal belang, de bescherming en bevordering van de Nederlandse waarden en buitenlandpolitieke doelstellingen', aldus de NDD.[17]

9 De *Militaire Spectator* bood tot nu toe plaats aan vier artikelen inzake *cyber warfare* en *cyber security*. Recent uitte de redactie zich via een Editoriaal over het belang van 'soft cyber' (het gebruik van sociale media e.d.): 'Cyber en militair vermogen', *Militaire Spectator* 181 (2012) (12) 530-531. Zie ook Graaf en Tettero (2010); Ducheine & Voetelink (2011-6); Akerboom (2012-12); en H-J van der Molen 'Cybersecurity - Relevante trends voor Defensie' (2013-03).

10 Doctrinair ingewijden kunnen deze uiteenzetting van het 'militaire denken' overslaan en volstaan met het bestuderen van figuur 2-4.

11 We baseren ons op de (in druk zijnde) nieuwe Nederlandse Defensie Doctrine (Concept d.d. maart 2013).

12 'Digitaal' en 'cyber' zullen we als synoniemen hanteren.

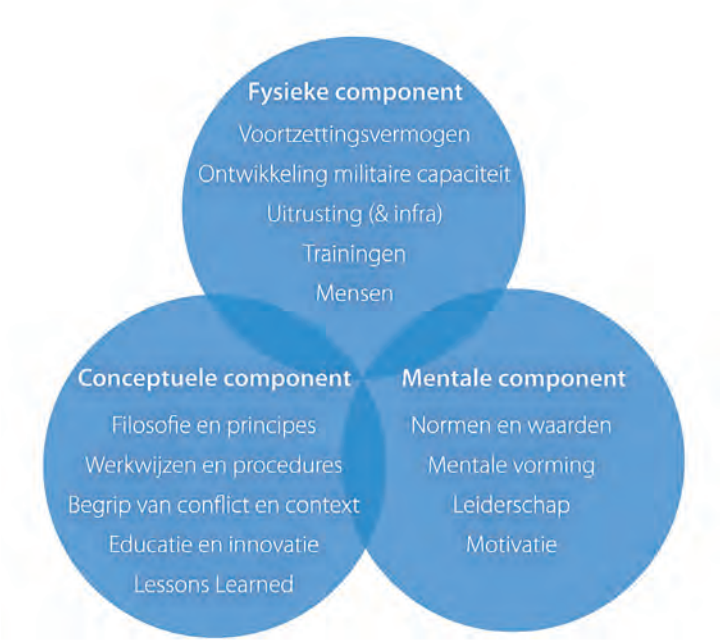
13 M.N. Schmitt (ed.). *Tallinn manual on the international law applicable to cyber warfare* (New York, Cambridge University Press, 2013) 258.

14 Waarbij we *warfare* (oorlogvoering) als fenomeen gebruiken. Voor een specifieke en beperkte betekenis: P.A.L. Ducheine, 'Legal Framework for Military Cyber Operations', in *Militair Rechtelijk Tijdschrift* 106 (2013) (1) 9-19.

15 Let wel: capaciteiten zijn middelen, *capabilities* is vermogen.

16 Ministerie van Defensie, *Nederlandse Defensie Doctrine* (2013) 21. Hierna: NDD (2013). Zie t.a.p. de alternatieve indelingen van machtsmiddelen/-instrumenten.

17 NDD (2013) 48.



Figuur 1. Militair vermogen

Het militaire machtsmiddel – de krijgsmacht dus – kan gedrag van andere statelijke en niet-statelijke actoren beïnvloeden via afschrikking, dwang en – ultimo – interventie met gebruik van geweld,[18] maar óók door samenwerking, training of (logistieke) steun.

Militair vermogen

De krijgsmacht genereert en levert militair vermogen (*fighting power*), omschreven als 'de totale capaciteit die de krijgsmacht levert om strategische functies te vervullen'.[19] Militair vermogen bestaat uit drie componenten: de fysieke, de conceptuele en de mentale (zie figuur 1).[20]

De fysieke component – gevechtskracht of *combat power* – bestaat allereerst uit 'personeel en materieel dat georganiseerd wordt ingezet in een operatie'.[21] Bij materieel moeten we denken aan goederen, infrastructuur, voer-, vaar- en vliegtuigen en uitrusting. Daarnaast behelst de fysieke component voortzettingsvermogen (*sustainability*) en operationele gereedheid (*readiness*).[22]

De mentale component bestaat uit factoren die onderling samenhangen: motivatie, leiderschap, mentale vorming, normen en waarden en tot slot 'perceptie van de toestand'.
Ter completering: doctrine, militair denken en principes, opleidings- en trainingsfilosofie vormen samen de conceptuele component.

De CDS beschrijft de synergie van de drie componenten van militair vermogen: 'Militair vermogen omvat meer dan uitsluitend de beschikbaarheid van operationele middelen (capacities). Men moet ook bereid en in staat (*capable*) zijn om deze middelen in te zetten. Als dit goed ontwikkeld is, dan spreekt men van militair vermogen (en worden *capacities* verheven tot *capabilities*)'.[23]

Militair vermogen wordt dus vanuit een strategische doelstelling, al dan niet samen met andere instrumenten van macht, aangewend om het gedrag van actoren te beïnvloeden.[24]

Aanwenden van militair vermogen

Militair vermogen wordt concreet doordat de krijgsmacht daadwerkelijke activiteiten, operaties genoemd, uitvoert. Operaties zijn divers in vorm, doelstelling, omvang en duur. Ze spelen zich af in verschillende domeinen: land, zee, lucht, (ruimte) en in het informatie- en digitale domein (zie hierna).

Schematische weergaven van het aanwenden van militair vermogen, oftewel een conceptueel model van operaties, kennen we bijvoorbeeld uit de *Land Doctrine Publicatie* II-C voor het optreden tegen irregulier optredende tegen-

18 NDD (2013) 22 en 41. In het Rapport Verkenningen wordt dit op een vergelijkbare wijze omschreven via (het gebruik van) strategische functies, bijvoorbeeld anticiperen, voorkomen, afschrikken, beschermen, interveniëren, stabiliseren, normaliseren. Ministerie van Defensie, *Eindrapport Verkenningen- Houvast voor de krijgsmacht van de toekomst* (2010)193.

19 NDD (2013) 71. Of zoals in NDD (2005) 50: 'de capaciteit om militaire operaties uit te voeren'.

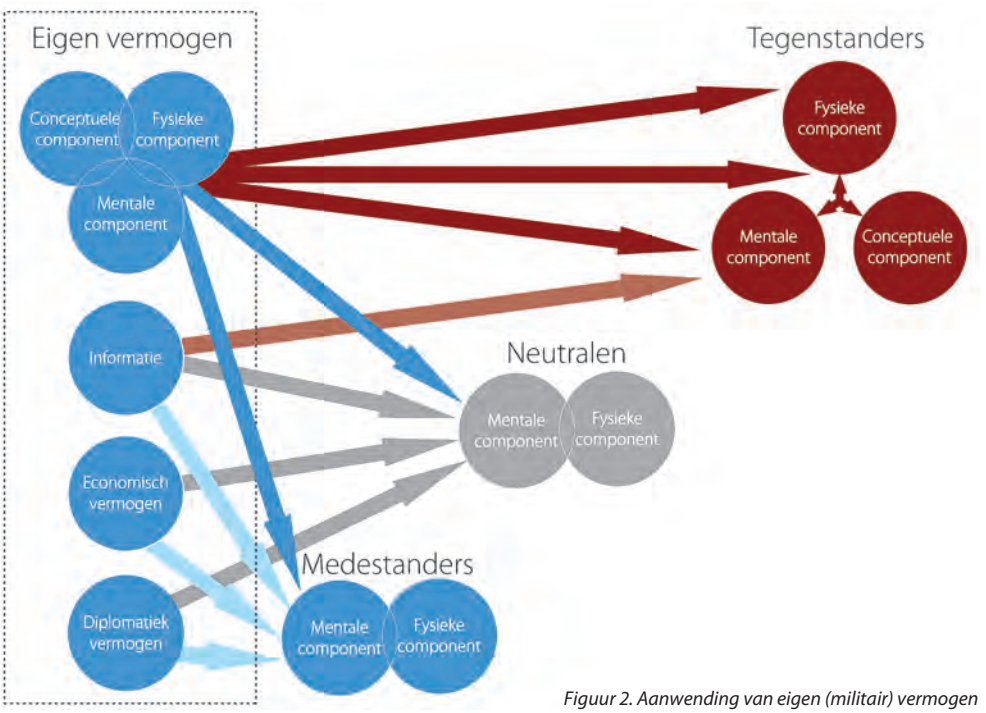
20 Naar de onderverdeling in: Koninklijke Landmacht, *DP 3.2 Landoperaties*, (concept versie 2.2, december 2012) 1-8. De onderverdeling verschilt per doctrinepublicaties: zie NDD (2013) 74, LDP-1 106, en DP 3.2 Landoperaties.

21 NDD (2013)77.

22 NDD (2005). Idem *DP 3.2 Landoperaties* 1-8/9.

23 NDD (2013)74, § 4.2.

24 Indien de instrumenten van macht in samenhang en gecoördineerd worden ingezet, mogelijk zelfs in internationaal verband, spreken we van een geïntegreerde benadering of *comprehensive approach*.



Figuur 2. Aanwending van eigen (militair) vermogen

standers.[25] We gebruiken dit model hier in een aangepaste vorm, die aansluit bij de manoeuvrebenadering en bij de geïntegreerde benadering.

De eerste aanpassing houdt in dat we naast tegenstanders ook medestanders en neutrale actoren toevoegen. Het beïnvloeden van actoren is een centrale notie. In de manoeuvrebenadering (*manoeuvrist approach*) wordt het eigen militaire vermogen vooral ingezet tegen onderkende zwakheden van andere actoren.[26] Operaties richten zich daarbij niet zozeer op de fysieke maar op de mentale component, en de samenhang tussen de drie componenten van het (militair) vermogen van anderen.[27] De nieuwe NDD verwoordt dit als volgt:

> *Effectief optreden wordt bepaald door benadering van alle actoren en niet alleen door de wijze waarop een tegenstander wordt benaderd. In het verlengde hiervan kan daarom de 'wil van de vijand' uit de traditionele manoeuvrebenadering worden gezien als de 'opinie van de actor'. De opinie vertaalt zich in steun en daarmee in samenhang ('cohesion'). Steun voor het eigen optreden moet worden behouden en vergroot. Steun voor de tegenstander moet worden beperkt, zodat hij uiteindelijk opgeeft. Door de eigen activiteiten gewogen af te stemmen op de 'will', 'understanding' en 'cohesion' van alle actoren, wordt invulling gegeven aan het denken in effecten en de manoeuvrebenadering in bredere zin.*[28]

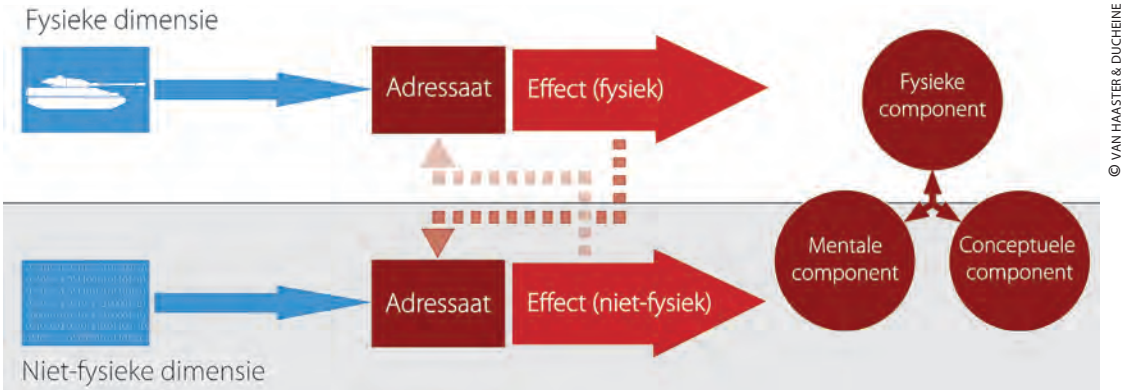
Figuur 2 visualiseert hoe het vermogen van tegenstanders, neutralen én medestanders wordt beïnvloed. Het belang van (aanvankelijke) neutrale partijen mag niet worden onderschat. Zo nam het aanvankelijk neutrale Anonymous onverwacht een zeer actieve rol aan in de Tweede Gazaoorlog en werd één van Israëls tegenstanders.

25 Koninklijke Landmacht, *Landmachtdoctrinepublicatie II-C: Gevechtsoperaties, gevechtsoperaties tegen een irregulier optredende tegenstander* (LDP II Deel C) (Zwolle, PlantijnCasparie, 2003) 529.

26 NDD (2013)120: 'Deze benadering is gericht op het beïnvloeden van de perceptie van de werkelijkheid, het gedrag en het optreden van actoren. Belangrijke aspecten hierbij zijn momentum, tempo en mentale beweeglijkheid (*agility*) die gecombineerd leiden tot een schokeffect en verrassing bij de actoren'.

27 NDD (2013)120-121.

28 NDD (2013)122.



Figuur 3. Middel-adressaat-effect

De inzet van machtsmiddelen zal er op gericht zijn dat deze neutrale partijen in ieder geval geen tegenstander worden: bij voorkeur medestander, maar minimaal neutralen.

Concreet betekent dit dat via operaties onder meer wordt getracht de samenhang tussen de componenten van het vijandelijke militaire vermogen te verbreken. Dit verbindende element is kwetsbaar en kan slechts in stand blijven bij de gratie van onder meer (de toegang tot) goede informatie.

Vervolgens wordt getracht de vijandelijke mentale component te degraderen en ten slotte (indien nodig) de vijandelijke fysieke component te reduceren. Vermogens van medestanders kunnen via de fysieke én de mentale lijn worden versterkt.

De tweede aanpassing van het model behelst het toevoegen van andere machtsinstrumenten, zoals diplomatiek vermogen en informatie, naast het militaire vermogen om actoren – tegenstanders, medestanders en neutralen[29] – via de geïntegreerde benadering te beïnvloeden.[30]

Het 'beïnvloeden' van tegenstanders met militaire middelen is vaak disruptief; we gebruiken ook wel de term 'aangrijpen'. Bij medestanders en neutralen is die beïnvloeding doorgaans constructief van aard.

Effecten en middelen

De daadwerkelijke activiteiten van de krijgsmacht leveren effecten op. In de aanwending van militair vermogen staan de manoeuvrebenadering en het denken in effecten, hun onderlinge relatie, hun relatie met actoren en de operationele omgeving centraal.[31]

De (beoogde) effecten zijn al dan niet fysiek van aard.[32] De daadwerkelijke vernietiging van een vijandelijk eskadron ligt in het fysieke vlak; 'breken' van de wil van deze eenheid ligt echter in het niet-fysieke, psychologische vlak. Fysieke effecten en psychologische effecten hebben meestal een wisselwerking op elkaar: zo kan de dood van een collega de wil breken van diens *buddy*.

De beoogde effecten worden met fysieke (harde) middelen, *hard power*, en niet-fysieke (zachte) middelen, *soft power*, gerealiseerd (zie figuur 3).[33] Een tank is een voorbeeld van een fysiek middel; informatie verstrekken of 'steun' is een voorbeeld van een niet-fysiek middel.

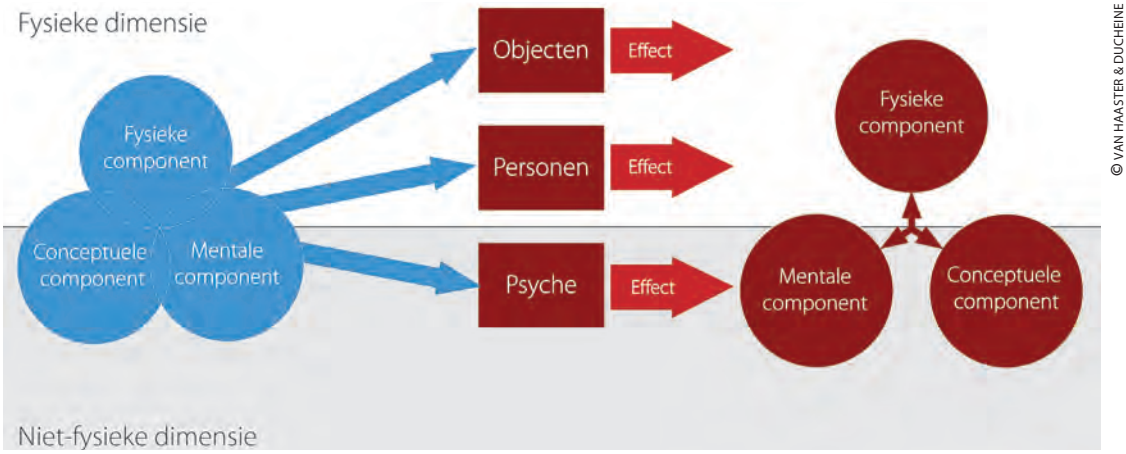
29 Zodat deze zich hetzij afzijdig dan wel als medestander op zullen (blijven) stellen.

30 *Comprehensive approach*: NDD (2013)29: 'Bij een geïntegreerde benadering worden de machtsmiddelen die een staat ten dienste staan, op gecoördineerde en samenhangende wijze ingezet, bij voorkeur in een coalitie met andere landen en in een samenwerkingsverband met internationale en niet-gouvernementele organisaties'.

31 *DP 3.2 Landoperaties*, 6-21.

32 NDD (2013) 117: 'Effecten kunnen zowel in het fysieke als het psychologische vlak worden bereikt'. Voor zover de effecten fysiek van aard zijn, betreft het zowel lethale als niet-letale effecten.

33 *DP 3.2 Landoperaties*, 4-6: 'Niet alleen de inzet van wapengeweld sorteert deze effecten. Beïnvloeding van tegenstanders door hun informatie en informatie-infrastructuur, hun financiële bronnen en hun draagvlak aan te tasten, is een bredere toepassing'.



Figuur 4. Middelen, adressaat en effecten

Het specifieke adressaat van militaire operaties, van middelen en methoden speelt een rol in het navolgende deel.

Adressaat

De vraag is tegen welke elementen van het (militaire) vermogen van andere actoren – tegenstanders, medestanders en neutralen – militaire operaties zich precies richten; wat is het aangrijpingspunt? We hanteren hiervoor zoals gezegd de term 'adressaat'.[34] Oftewel: waartegen worden fysieke en niet-fysieke middelen (hard en soft power) ingezet om effecten in het fysieke en/of het psychologische vlak te realiseren?
De fysieke component kan worden aangegrepen via mensen en objecten (zie figuur 4).

'Mensen' betreft zowel individuen als groepen die deel uitmaken van (potentiële) tegenstanders, neutralen en medestanders (inclusief de eigen troepen en bevolking). Bij 'objecten' gaat het om fysiek tastbare goederen zoals uitrusting, materieel, logistieke voorraden en infrastructuur (zie ook figuur 1).

Het beïnvloeden van de mentale component geschiedt via de 'psyche', oftewel door het beïnvloeden van motivatie, wil, gevechtsbereidheid en de effectiviteit van leiderschap via het overbrengen van informatie, signalen, indrukken, et cetera. Daarnaast wordt de perceptie van de situatie of het begrip van de toestand beïnvloed. Die effecten zijn niet-fysiek.

De samenhang tussen de drie componenten van (militair) vermogen kan worden aangegrepen door cruciale onderdelen van leiderschap, besluitvorming en bevelvoering, commandovoeringsondersteuning en informatieverwerking (objecten, informatie en processen) uit te schakelen of te beïnvloeden. Uiteindelijk valt dit ook terug te voeren op generieke adressaten: mensen, objecten en psyche.

Een belangrijk gegeven is de wisselwerking tussen fysieke en niet-fysieke aangrijpingspunten en effecten (zie terug).

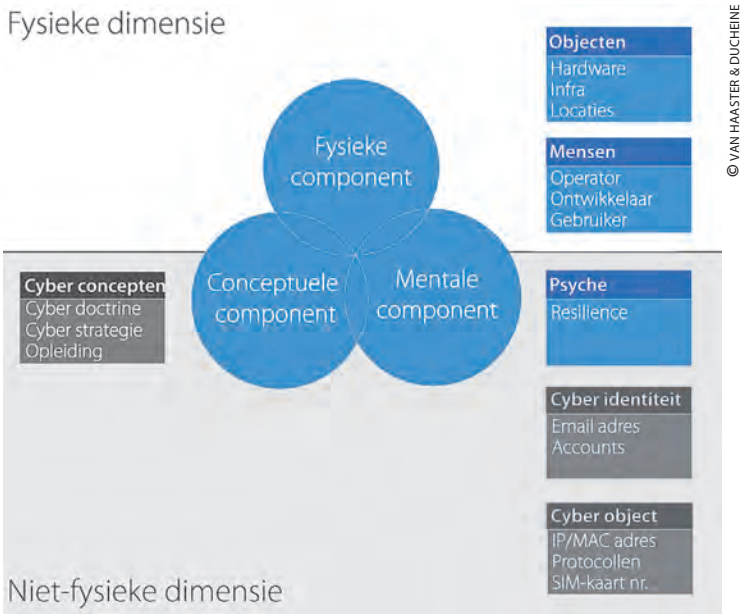
Effecten

Effecten worden in verschillende dimensies (fysiek en niet-fysiek) via militaire operaties – solitair of geïntegreerd, *joint* en/of *combined* – gerealiseerd.[35]
De fysiek bepaalde domeinen land, zee, lucht (en ruimte) zijn qua middelen te koppelen aan de fysieke dimensie, terwijl de gewenste effecten zowel in het fysieke als in het niet-fysieke vlak kunnen liggen.

We zullen deze doctrinaire inzichten hierna aanvullen met het digitale domein en digitale

34 Om verwarring met de LDP-1 (99) te voorkomen, gebruiken we hierna alleen de term 'adressaat'.

35 *Joint*: verschillende krijgsmachtdelen werken samen; *combined*: krijgsmachten van verschillende staten werken samen.



Figuur 5. Cyber capabilities en militair vermogen

operaties.[36] We besteden daarbij aandacht aan cyber-operaties en hun beoogde effecten, beschikbare middelen en methoden en het adressaat.

Het digitale domein

De eerste vraag is uiteraard: wat is het digitale domein of cyberspace? Het digitale domein onderscheidt zich van de andere domeinen doordat het niet geografisch of fysiek afgebakend is. Dit betekent overigens niet dat het digitale domein of cyberspace geen fysieke elementen bevat. Integendeel. Het digitale domein wordt gedefinieerd als 'het geheel van ICT-middelen en ICT–diensten'.[37] Dit domein bestaat ook uit 'alle niet met internet verbonden netwerken of andere digitale apparaten'.[38]
Los van deze definitie is het natuurlijk de eerste vraag hoe cyberspace er uitziet.

Het digitale domein heeft een aantal 'lagen' of onderdelen. Voor het doel van deze bijdrage volstaat een tweedeling: een fysieke en een niet-fysieke laag.[39] De fysieke laag bestaat uit geografische locaties en fysieke objecten zoals hardware (computers, *servers, routers, smartphones*) en hun fysieke verbindingen (zoals glasvezelkabels, zendmasten).[40] Tot de fysieke dimensie rekenen wij ook mensen: de gebruikers en bedienaars van de middelen en capaciteiten binnen dit domein.[41]

Het unieke van het digitale domein ligt in de tweede, de virtuele laag (*logical layer*), bestaande uit protocollen, software en digitale verbindingen tussen fysieke knooppunten en onderdelen in het netwerk.[42] Bovendien bevat deze laag de applicaties en software binnen de onderdelen van het netwerk zelf. Deze laag bevat eveneens data in de vorm van de cyber-identiteiten van mensen (e-mailadressen, digitale accounts op *Facebook, Linkedin*, gsm-telefoonnummers) en cyber-objecten (zoals IP-adressen, MAC-adressen en SIM-kaartnummers).[43]
Deze virtuele laag maakt het mogelijk dat de objecten en personen binnen een fysieke netwerkinfrastructuur met elkaar kunnen communiceren en dat data-overdracht mogelijk is.[44]

36 Cyberspace wordt (al dan niet terecht) het vijfde domein genoemd. Zie onder meer NATO (2010) AJP 01d, 5-14 en NDD (2013) 81.
37 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV, 2011): *Digitale oorlogvoering*, Den Haag: AIV no. 77; CAVV no. 22, zie <www.aiv-advice.nl>, bijlage III.
38 AIV/CAVV (2011), bijlage III.
39 De niet-fysieke laag bestaat weer uit meerdere sub-lagen. Het OSI model hanteert zeven lagen: de fysieke laag, de datalink-laag, de netwerklaag, de transportlaag, de sessielaag, de presentatielaag en de applicatielaag. Het gelaagde OSI model wordt wereldwijd gebruikt als referentiemodel voor netwerkcommunicatie, zie: <www.tekstenuitleg.net/artikelen/netwerken/osi-model/osi-model.html>. TCP/IP hanteert vier lagen: applicatielaag, transportlaag, internetlaag, network interface, zie <technet.microsoft.com/nl-nl/library/cc786900(v=ws.10).aspx>. Drie lagen komen terug in: United States Army Training and Doctrine Command (TRADOC 2010), *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet 525-7-8, <www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf>, 8. Zie ook L. Tabansky, 'Basic Concepts in Cyber Warfare', in: *Military and Strategic Affairs* 3 (2011)(1), 75-92, 78.
40 TRADOC (2010) 8.
41 In sommige indelingen maken personen (en hun cyber-indentiteit) deel uit van een derde laag: de sociale laag. Zie bijvoorbeeld TRADOC (2010) 9.
42 TRADOC (2010) 9.
43 Internet Protocol (IP)-adressen, Media Access Control (MAC)-adressen, Subscriber Identity Module (SIM) -kaart.
44 Let wel: *DP3.2 Landoperaties* typeert het elektromagnetische spectrum als een fysiek fenomeen: 4-6, § 4213.

De niet-fysieke virtuele laag met de daarin besloten liggende capaciteiten en risico's maakt cyberspace bijzonder.

Het digitale domein en militair vermogen
De volgende vraag is welke cyber-elementen bijdragen aan militair vermogen. We analyseren dit voor de fysieke, de mentale en de conceptuele componenten (zie figuur 5). Daarbij doet zich een indelingsvraagstuk voor omdat een aantal niet-fysieke elementen van cybervermogen zich lastig laat onderbrengen in de klassieke driedeling.

Fysieke component
De fysieke laag van het cyber-domein rekenen we tot de fysieke component van militair vermogen: het gaat – net als in de normale wereld – op de eerste plaats om objecten en mensen. De objecten betreffen alle knooppunten in het netwerk (hardware zoals routers, servers en computers),[45] fysieke verbindingen (zoals glasvezel- of koperkabel) en objecten voor niet-kabelgebonden verbindingen (zendmasten e.d.) tussen de knooppunten.[46]

'Mensen' betreft allereerst operators, bedienaars van de objecten en daarnaast gebruikers in het digitale domein, bijvoorbeeld twitteraars en volgers, alsmede softwareontwikkelaars en hackers (in overheidsdienst).

Naar analogie van het reguliere fysieke vermogen noemen we ook cyber-oefeningen, oefenfaciliteiten en de ontwikkeling van cyber-capaciteit.[47] Daar hoort onder meer een 'oefenlaboratorium' bij: een veilige testomgeving om met digitale 'wapens' en methoden te oefenen.[48]

Virtuele afspiegeling van fysieke elementen
Mensen en objecten in het cyber-domein moeten kunnen communiceren, waarvoor gebruik wordt gemaakt van software, applicaties, accounts en protocollen uit de virtuele laag. Dat levert, zoals gezegd, een indelingsprobleem op, dat we nu zullen adresseren.

De virtuele afspiegeling van objecten en mensen rekenen we niet tot de fysieke component van

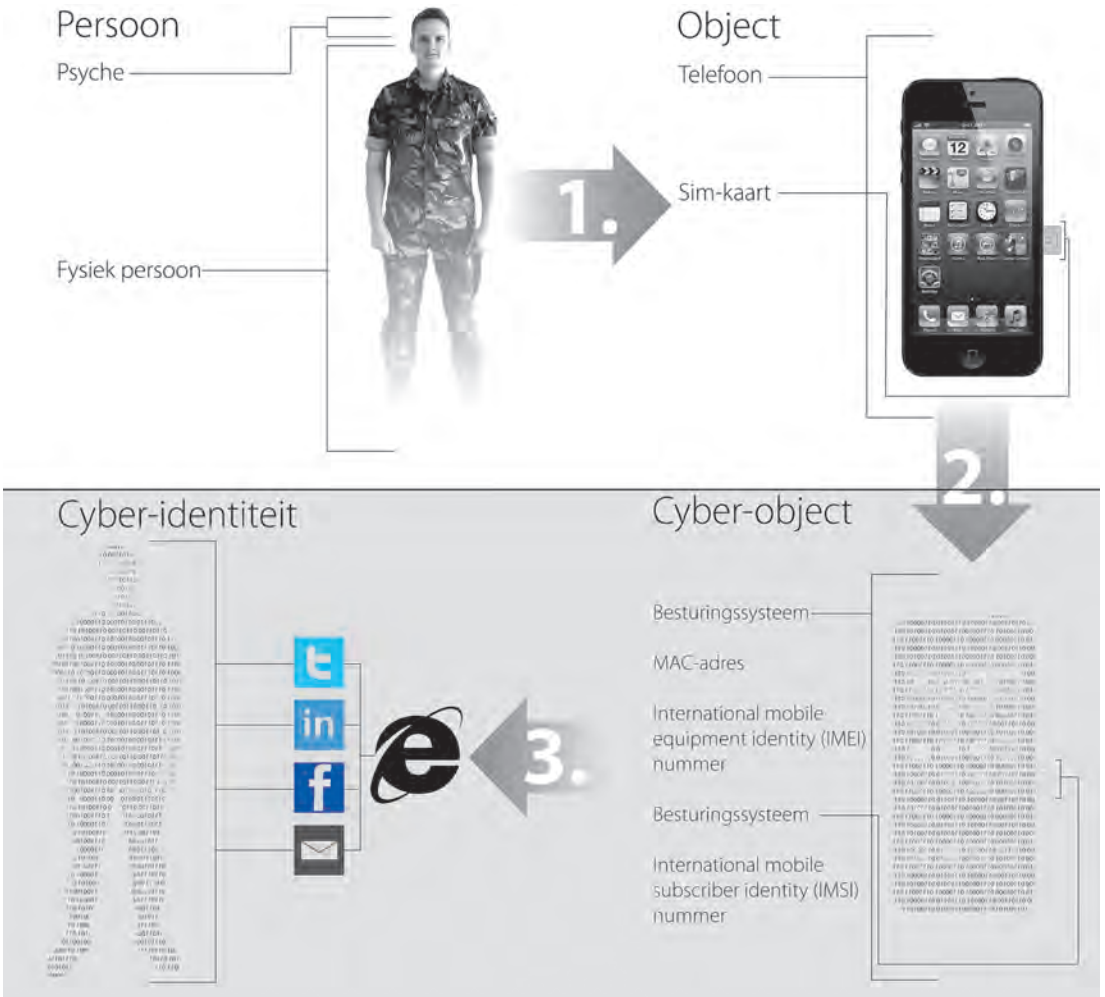
Figuur 6. De cyber-identiteit van Jeanine Hennis-Plasschaert (https://twitter.com/JeanineHennis/status/268006560788254722

militair vermogen. Ze zijn immers niet fysiek, niet tastbaar. Het gaat 'slechts' om een reflectie van fysieke onderdelen. Het zijn virtuele elementen die onlosmakelijk – maar niet één op één – te relateren zijn aan fysieke objecten en mensen. We noemen deze cyber-objecten en cyber-identiteiten.

Zoals gezegd faciliteert de virtuele laag van het digitale domein de fysieke laag zodat communicatie mogelijk is. De logical layer bestaat uit verschillende cyber-objecten: virtuele onderdelen zoals software, protocollen (bijvoorbeeld Internet Protocol of IP)[49], processen (e-mail, encryptie, *Domain Name System*), adressen (bijvoorbeeld IP- en MAC-adressen, SIM-kaart nummers)[50] en overige data (zoals besturingssystemen).[51]

Mensen én wat we hun psyche hebben genoemd (wat op zich al een virtueel aspect is)

45 TRADOC (2010), 9.
46 J. Andress & S. Winterfeld, Cyber Warfare: *Techniques, Tactics and Tools for Security Practitioners* (Waltham, Syngress, 2011) 120.
47 Bijvoorbeeld de oefening *Locked Shield* 2013, waarbij het Nederlandse team de derde plaats behaalde. Zie: http://www.ccdcoe.org/401.html .
48 Zie voor een omschrijving van basiswaarborgen voor fysieke netwerkinfrastructuur: C.P. Pfleeger & S.L. Pfleeger , *Security in Computing* (4th Ed.) Prentice Hall, 2007, 442-443.
49 Ook: OSI, IPv4/6, http, HTML, TCP, UDP.
50 IP-adres: een nummer voor een internetaansluiting voor hardware. MAC-adres: uniek nummer van hardware.
51 Pfleeger & Pfleeger (2007) 385-386.



Figuur 7. Relatie personen, objecten en cyber-objecten en cyber-identiteiten.

kennen ook een virtuele equivalent in het cyber-domein: de cyber-identiteit (of *cyber personality*). Steeds meer sociale en beroepsmatige aspecten van mensen spelen zich af in het cyber-domein,[52] zoals via sociale media.[53] Veel mensen hebben, om bereikbaar en verbonden te zijn, informatie online staan en beschikken over een of meerdere *cyber-identiteiten*. Cyber-identiteiten bestaan uit profielgegevens op sociale media, mailadressen, blogs en alle andere data die online staan en gelieerd zijn aan een bepaald persoon (zie figuur 6). Twitter- en Facebook-accounts zoals *@Landmacht* of <*www.facebook.com/Commandantderstrijdkrachten*> zijn sprekende voorbeelden.[54]

Overigens kan één persoon meerdere identiteiten hebben, één identiteit kan meerdere personen betreffen en sommige identiteiten representeren niet wat ze suggereren: *@Koning_NL*, *@MinisterHennis* en

52 C.L. Coyle & H. Vaughn, 'Social networking: Communication revolution or evolution?', in: *Bell Labs Technical Journal* 13 (2008)(2)13-17; S. Matthews, 'On-line Professionals', in: *Ethics and Information Technology* 8 (2006) 66; M. Miller & D. Slater, *The Internet: An Ethnographic Approach* (Oxford, Berg. Chapter One – Conclusions, 2006); Antoci et al., *See you on Facebook: the effect of social networking on human interaction*, (European Research Institute on Cooperative and Social Enterprises, 2010) 182.

53 Antoci (2010); PCCLM (2011), *A Survey on What Content do People Share Online and With Whom?* <pcclm.com/2011/05/survey-on-what-do-people-share-content.html>.

54 Zie 'Cyber en Militair Vermogen', in: *Militaire Spectator* 181 (2012)(12) 530-531.

Toelichting figuur 7
In de fysieke laag treffen we een persoon en een fysiek object met internetverbinding, bijvoorbeeld een smartphone, waarmee hij toegang heeft tot de cyberspace (stap 1).[a] De telefoon bestaat uit twee relevante fysieke onderdelen: een SIM-kaart[b] en het toestel zelf. Deze fysieke objecten hebben een digitale representatie in de virtuele laag via drie cyber-objecten (stap 2). Allereerst het International Mobile Equipment Identity (IMEI)-nummer dat gekoppeld is aan het toestel. Daarnaast heeft het toestel een MAC-adres dat gebruikt worden om het toestel binnen een netwerk te identificeren en dataoverdracht te faciliteren. Op de derde plaats het International Mobile Subscriber Identification (IMSI)-nummer dat de gebruiker als abonnee identificeert.[c] Het ISMI- nummer is opgeslagen op de SIM-kaart die de gebruiker bij het afsluiten van een vast abonnement of bij aanschaf van een 'beltegoed' variant in bezit krijgt.[d]
De fysieke objecten (smartphone en SIM-kaart) én de cyber-objecten (IMEI-, IMSI-nummer en MAC-adres) faciliteren de gebruiker en diens virtuele manifestaties: de cyber-identiteiten (stap 3). Via zijn IMSI-nummer kan hij gebruik maken van internet en zijn cyber-identiteiten opbouwen via online services zoals Twitter en e-mail.

a Vanwege de overzichtelijkheid hanteren we slechts de mannelijk aanduiding of verwijzingsvorm: hij/zijn.
b *Subscriber Identity Module* (SIM) is een smartcard waarop de gegevens staan van een aansluiting/abonnee van een mobiele telefoon.
c *MSI identificeert een gebruiker via een SIM-kaart of IMEI-nummer.* Zie www.princeton.edu/~achaney/tmve/wiki100k/docs/International_Mobile_Subscriber_Identity.html.
d IMEI identificeert een toestel..

<*www.facebook.com/gentom.middendorp*> zijn 'nep' accounts.[55]
In figuur 7 hebben we de relatie tussen de fysieke en de virtuele dimensie uiteengezet en demonstreren we hoe de virtuele representatie van fysieke elementen werkt in het geval van een smartphone.

Conceptuele en mentale component
Net als andere operaties zullen ook cyber-operaties doctrinair worden voorbereid en uitgevoerd. De doelstelling van onze bijdrage sluit daarbij aan: doctrine, grondbeginselen en principes, lessen, opleidings- en trainings-filosofie op het concept cyber warfare en zijn implicaties moeten worden doorgrond. Uiteraard moet dit vervolgens in opleidingen worden geïncorporeerd. Via eerder genoemde trainingen en oefeningen (zie de fysieke component) draagt dit bij aan het militaire vermogen als geheel. Het personeel dient ook gemotiveerd te zijn en over een militaire *mindset* te beschikken waardoor het in staat is en blijft de cyber-doctrine uit te voeren.[56] Deze aspecten vinden we terug in de conceptuele en de mentale component.

De samenhang tussen de drie componenten alsmede de integratie van cyber-operaties en -capaciteiten in andere onderdelen van militair vermogen, in operaties én in andere machts-instrumenten, moet eveneens worden doordacht. Militaire planners moeten bekend zijn met de samenhang tussen de verschillende lagen van cyberspace. Dat heeft, met andere woorden, invloed op de conceptuele en mentale component. Ook de interactie tussen sociale, technische en operationele (militaire) processen moet kunnen worden begrepen en gehanteerd. Met cyber warfare zet de krijgsmacht andermaal stappen in de niet-kinetische dimensie, een ontwikkeling die herkenbaar is uit recente COIN-ervaringen.

Wat nu reeds opvalt is het feit dat het digitale domein een niet-fysieke laag met virtuele capaciteiten heeft: cyber-objecten en cyber-identiteiten. Is dit volstrekt nieuw? Enerzijds niet als we het 'denken in effecten' en de inzet van 'soft power' in ogenschouw nemen. In dat opzicht vormen deze virtuele (cyber-) capaciteiten slechts een uitbreiding. Anderzijds is hiermee sprake van volstrekt nieuwe elementen, dito capaciteiten en mogelijkheden, maar ook nieuwe risico's.

55 Idem: *@WillemAlexander*, zie <twitter.com/WillemAlexander>.
56 Een militaire *mindset*: zie A. Benschop, *Cyberoorlog* (Tilburg, Uitgeverij de Wereld, 2013). Voor een omschrijving van de '*cyber warrior*': Andress & Winterfeld (2011)61-69.

Zelfs al zou dit geen doctrinaire gevolgen hebben, het enkele feit dat cyber-identiteiten en cyber-objecten bestaan, is relevant voor doctrinair denken. Deze extra mogelijkheden (en kwetsbaarheden) vragen om bewustwording, acceptatie en adaptatie van de virtuele dimensie en de samenhang met de fysieke. Cyber warfare is meer dan 'het aanvallen van een hacker' of het 'targeten van een server', zoals regelmatig wordt gehoord.

Een ander markant feit is de relatie tussen cyber-operaties en informatieoperaties.[57] We volstaan hier met de opmerking dat cyber-operaties qua principe informatieoperaties volgen, maar qua adressaat een unieke positie innemen. Ook 'soft cyber'-operaties zijn daardoor afwijkend ten opzicht van gangbare informatieoperaties.

Een laatste factor van invloed is de rol en betekenis van geografie en ruimte in cyberspace. Deze is anders dan bij louter kinetische operaties. Actoren (en fysieke objecten die deel uitmaken van het cyber-domein) kunnen zich overal ter wereld bevinden. Dit wil niet zeggen dat cyber warfare ontdaan is van fysieke grenzen. Sterker nog, deze spelen nog steeds een belangrijke rol: objecten en mensen bevinden zich namelijk in de fysieke laag. Maar met internet als vector en het gebruik van cyber-objecten en cyber-identiteiten, zijn afstanden erg kort, en de 'ruimte' waarin operaties plaatsvinden ('het slagveld') erg groot. Hoewel de virtuele elementen tot fysieke onderdelen zijn te herleiden, kan de geografische locatie daarvan weer complicaties opleveren indien cyber-operaties worden overwogen.[58]

Cyber in militair vermogen

Doordachte integratie van cyber-capaciteiten in andere onderdelen van militair vermogen, in operaties én in andere machtsinstrumenten, is een vereiste. Cyber capabilities vinden we in de vertrouwde fysieke, conceptuele en mentale component van (militair) vermogen, namelijk personen (inclusief groepen en militaire eenheden), objecten (inclusief fysieke netwerkinfrastructuur) en de psyche.

De unieke toegevoegde waarde is gekoppeld aan de virtuele laag van het digitale domein, waarin de nieuwe capaciteiten cyber-identiteiten en cyber-objecten besloten liggen. Deze onderdelen faciliteren de exploitatie van het cyber-domein. Hierna gaan we in op de concrete invulling van cyber-operaties.

Cyber-operaties

In onze inleiding definieerden we cyber-operaties als 'de inzet van cyber capabilities met het primaire (militaire) doel in of via cyberspace effecten te realiseren'.[59] Uiteindelijk dienen ook cyber-operaties een hoger (strategische bepaald) doel: het beïnvloeden van actoren in of via cyberspace.

Beïnvloeding 'in of via cyberspace' impliceert twee parallelle noties. Enerzijds worden effecten via cyberspace gerealiseerd. Cyberspace fungeert als vector voor een cyber-middel en biedt derhalve (ook) ruimte voor het gebruik van social media (zie hierna). Anderzijds worden effecten in cyberspace gerealiseerd: in de fysieke en/of de virtuele laag. Dit betreft bijvoorbeeld de inzet van software tegen luchtverdediging.

Cyber-operaties kunnen op zichzelf staan, of deel uitmaken van andere (kinetische) operaties.[60] Net als in Nederland beogen meerdere staten cyber-operaties te integreren in hun reguliere militaire operaties.[61] Dat laatste was bijvoorbeeld zichtbaar bij

57 NDD (2013)101.

58 Zie: P. Ducheine, J. Voetelink, J. Stinissen & T. Gill, 'Towards a Legal Framework for Military Cyber Operations', in: Ducheine, Osinga & Soeters (eds.), *Cyber Warfare: Critical Perspectives* (2012)101-128.

59 Schmitt (2013) *Tallinn manual*, 258: 'The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'.

60 T. Gill & P. Ducheine, 'Anticipatory Self-Defence in Cyber Warfare', in: M. Schmitt (Ed.), *Cyber War and International Law* (International Law Studies 2012, Newport: Naval War College Press) <www.usnwc.edu/Publications/International-Law-Studies-(1).aspx>.

61 Voor nationale militaire cyber -doctrines: E. Tikk (2011) *Frameworks for International Cyber Security, National Cyber Security Policies and Strategies*, via <www.ccdcoe.org/284.html>. Zie D. Cameron (2010), *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Rewiev* 27 (2010), via <www.official-documents.gov.uk/document/cm79/7948/7948.asp>: 'Future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land and air environments'.

operatie *Orchard* in september 2007, waarbij (vermoedelijk) Israël een luchtaanval uitvoerde op een Syrische nucleaire installatie in Al-Kibar.[62] Daarbij is de Syrische luchtverdediging met een parallelle cyber-operatie (tijdelijk) gemanipuleerd.[63]

In de literatuur worden cyber-operaties vaak beschreven via een fasering waarin verschillende (deel)doelstellingen herkenbaar zijn.[64] Cyber-operaties kunnen – afhankelijk van de doelstelling – deze gehele fasering (zie figuur 8: operatie C) of slechts een deel daarvan omvatten. Afhankelijk van het beoogde effect zullen bepaalde cyber-capaciteiten in specifieke fases worden ingezet. Zo bestaat er een middel (i.c. software) om kwetsbaarheden in netwerken te 'scannen' zodat een toegang tot een systeem gevonden kan worden (zie figuur 8: operatie A). Andere software verzamelt – na intrusie – in een netwerk informatie (idem: operatie B). Anders gezegd: los van én binnen dit generieke model bestaat een diversiteit aan cyber-capaciteiten die voor verschillende (deel)doelstellingen zijn in te zetten.

In beginsel staat niets in de weg om cyber-operaties ook via de manoeuvrebenadering en de geïntegreerde benadering vorm te geven. Sterker nog, gelet op de immer toenemende digitale afhankelijkheid van mensen en organisaties ligt een digitaal 'aangrijpingspunt' voor de hand.[65]
Hoe deze operaties nu precies vorm krijgen, bezien we hierna door achtereenvolgens in te gaan op adressaat, effecten en middelen/methoden bij cyber-operaties.

Adressaat en effecten
Cyber-operaties richten zich – via een adressaat – op tegenstanders, medestanders en neutralen en wel op de cyber capabilities in het (militaire) vermogen van die actoren. Hiervoor benoemden we die capabilities: personen, objecten en psyche alsmede de virtuele afspiegelingen cyber-objecten en cyber-identiteiten.
Directe effecten van cyber-operaties liggen in de niet-fysieke dimensie door 'contact' in de virtuele laag met cyber-objects en cyber-identiteiten. Bijvoorbeeld omdat een cyber-object niet meer functioneert.

Cyber-operaties steunen daarnaast op indirecte, secundaire effecten - zowel in het fysieke als niet-fysieke vlak.[66] Mensen en objecten in de

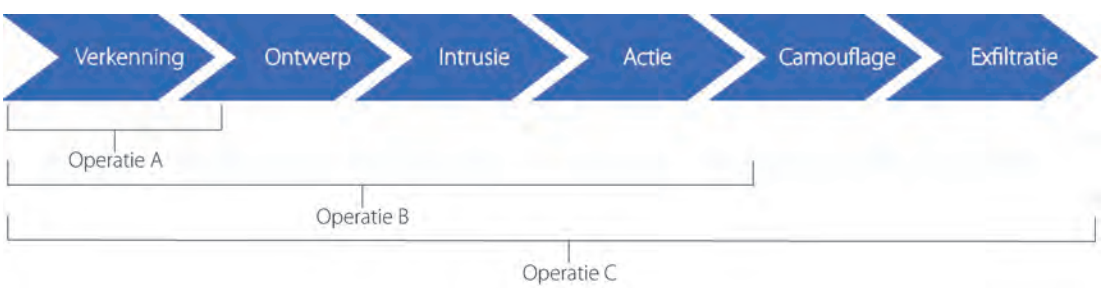
62 A. Garwood-Gowers, 'Israel's Airstrike on Syria's Al-Kibar Facility: a Test Case for the Doctrine of Pre-Emptive Self-Defence?', in: *Journal of Conflict & Security Law* 16 (2) 263-291: D. Gartenstein-Ross & J.D. Goodman (2009), 'The Attack on Syria's al-Kibar Nuclear Facility', in: *Focus Quarterly*, Spring, via <www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility>; BBC News (Oct. 2, 2007), 'Israel admits air strike on Syria', via <news.bbc.co.uk/2/hi/middle_east/7024287.stm>.

63 D.A. Fulghum & D. Barrie (2007), 'Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target', in: *Aviation Week* (8-10-2008) 28, via: <www.freerepublic.com/focus/f-news/1908050/posts>.

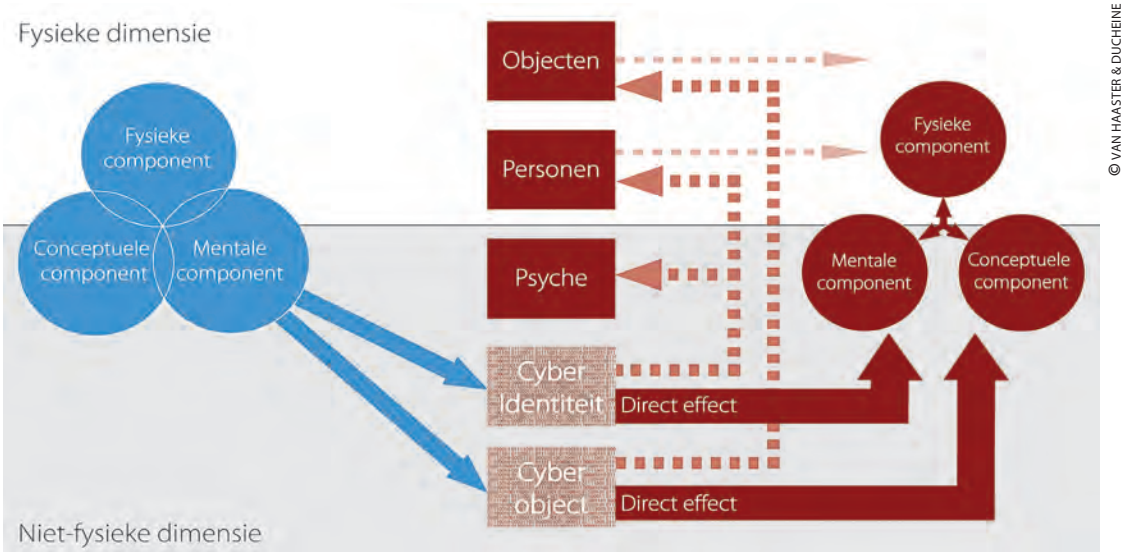
64 Zie: Andress & Winterfeld (2011)171: Reconnaisance, scan, access, escalate, exfiltrate, assault, sustain; Janczewski & Colarik (2008), Verkenning, binnendringen, uitbreiden, actie, bewijs verwijderen); Grant, Venter & Eloff (2007), *Footprinting, reconnaissance, vulnerability identification, penetration, control, embedding, data extraction or modification, attack relay, attack dissemination*.

65 Zie ook Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999, via <m.tech.uh.edu/faculty/conklin/IS7033Web/7033/Week2/unrestricted.pdf>, 199: 'One hacker + one modem causes an enemy damage and losses almost equal to those of a war'.

66 W.A Owens, K.W. Dam, & H.S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington D.C., National Academic Press, 2009) 127.



Figuur 8. Generieke fasering in cyber-operaties



Figuur 9. Adressaat in cyber-operaties

fysieke dimensie worden indirect beïnvloed door operaties tegen cyber-identiteiten en cyber-objecten. Dat geldt ook voor de samenhang. Door operaties tegen bijvoorbeeld cyber-objecten van communicatiesysteem kan een *common operational picture en situational awareness* van de tegenpartij verstoord of verdraaid worden, waardoor de samenhang in vermogen gedegradeerd wordt.

De psyche van mensen wordt indirect beïnvloed door cyber-objecten aan te grijpen en cyber-identiteiten te manipuleren. Bijvoorbeeld door mobiel internet te ontregelen en nepberichten aan bestaande accounts toe te voegen. We hebben deze (in)directe effecten in figuur 9 gevisualiseerd.

Middelen en effecten

Effecten van cyber-operaties treden zoals gezegd uiteindelijk op in de fysieke én niet-fysieke lagen van cyberspace. De beoogde effecten van (delen van) cyber-operaties wisselen naargelang de doelstelling. Het betreft een breed spectrum, variërend van het verbeteren van informatieposities tot disruptieve acties zoals Stuxnet.[67]

Ter illustratie van dit spectrum – en zonder compleet te willen zijn[68] – beschrijven we middelen en methoden die tegen cyber-identiteiten en cyber-objecten kunnen worden ingezet. De mate van detaillering wijkt af van het voorgaande deel: dat heeft als doel deze relatief onbekende materie met voorbeelden te illustreren.

Waar nodig maken we onderscheid tussen tegenstanders, medestanders en neutralen: de beoogde effecten houden verband met de aard van deze drie groepen. Anders gezegd: bij medestanders zullen vaak constructieve effecten beoogd zijn; bij tegenstanders disruptieve.

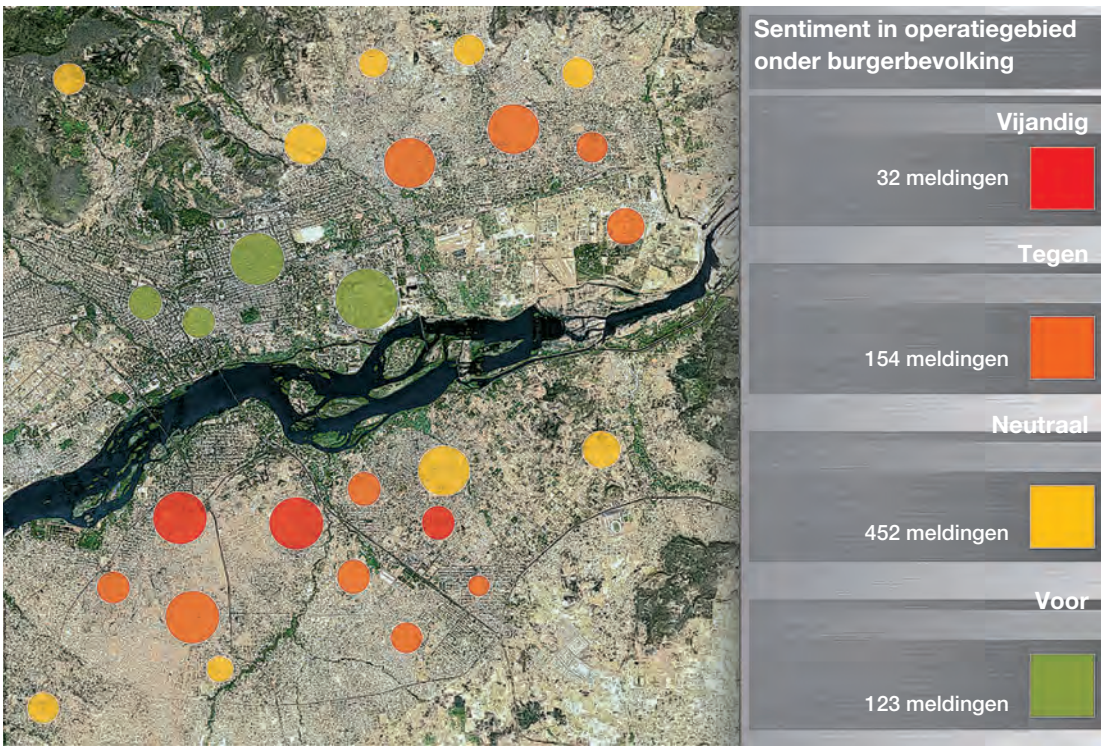
Exploitatie van cyber-identiteiten

Het feit dat een groot deel van de samenleving – individuen en groepen – een cyber-identiteit heeft, deze (actief) gebruikt en daar steeds afhankelijker van wordt,[69] maakt het interessant over capaciteit(en) te beschikken om deze te exploiteren.

67 Zie o.a. H.S. Lin, 'Offensive Cyber Operations and the Use of Force', in: *Journal of National Security Law & Policy*, 4 (2010) 63-85; T. Rid & P. McBurney (2012) 'Cyber-Weapons', in: *The RUSI Journal* 157(1) 6-13. Tabansky (2011).

68 Technologische ontwikkeling en voorstellingsvermogen begrenzen de potentiële mogelijkheden en middelen.

69 Zie het voorbeeld van het betalingsverkeer uit de inleiding. Zie ook F. Osinga, 'Introducing Cyber Warfare', in: Ducheine, Osinga & Soeters (eds.) *Cyber Warfare – Critical Perspectieves* (2012)1-18.



Figuur 10. Datamining

Exploitatie kan bestaan uit het verzamelen van informatie (a), het verspreiden van informatie (b) en/of het impliciet of expliciet beïnvloeden van personen – medestanders, tegenstanders of neutralen – zowel thuis of in een operatiegebied (c). Indien cyber-identiteiten digitaal toegankelijk zijn kunnen deze ook gemanipuleerd of vernietigd worden (d).

● *Informatie verzamelen*

Cyber-identiteiten kunnen worden benaderd om informatie te verzamelen, waardoor een beeld kan worden gegenereerd van het sentiment van individuen, van groepen en de samenleving. De informatie over cyber-identiteiten bevindt zich in open bronnen (*social-networking sites*, blogs en dergelijke) en in niet-openbare bronnen (mailverkeer e.d.).

Informatie verzamelen over één individu is niet arbeidsintensief; over een samenleving of operatiegebied daarentegen wel. De hoeveelheid beschikbare data maakt het lastig de 'juiste' informatie te vinden. Ter illustratie: per minuut worden 684.478 Facebook-berichten gedeeld, 100.000 Tweets gepost, 3.600 *Instagram*-foto's geplaatst, 347 nieuw *Wordpress*-blogs aangemaakt en 48 uur video via *YouTube* geüpload.[70]

Om uit deze overvloed relevante informatie te kunnen destilleren, is software ontwikkeld die het sorteren, aggregeren, correleren, clusteren en *geo-taggen* van open informatie ondersteunt.[71] Met deze *datamining tool*' kan een beeld gegenereerd worden van het sentiment in het thuisland of operatiegebied via de cyber-identiteiten (zie figuur 10).[72]

Om niet-openbaar informatie van cyber-identiteiten te verkrijgen zijn andere, meer invasieve methoden nodig. Bijvoorbeeld door dataverbindingen af te luisteren of af te tappen,

70 N. Spencer (2012) 'How Much Data is Created Every Minute?' via: <visualnews.com/2012/06/19/how-much-data-created-every-minute/>.

71 Pfleeger & Pfleeger (2007) 367.

72 Ter illustratie van de werking in thuisland: <nederlandsespoorwegen.crowdmap.com>.

Figuur 11. Tweet op zoek naar draagvlak en geld

door gebruikers te verleiden c.q. te misleiden tot het afgeven van toegangsgegevens: *social engineering* genaamd. Of door in te breken (hacken) in accounts.[73] Bij één persoon is de benodigde tijd te overzien; een (bevolkings-) groep 'handmatig' afluisteren is zeer arbeidsintensief.

Inlog- en accountgegevens zouden op grote(re) schaal kunnen worden achterhaald door twee vormen van social engineering: *phishing* of *pharming*.[74] De doelgroep krijgt bijvoorbeeld een legitiem ogend bericht waarin een gebruiker gevraagd wordt in te loggen op een clandestiene website (*pharming*) of een bijlage te openen, waardoor diens computersysteem gecompromitteerd wordt (*phishing*).[75] De inloggegevens die dit zou opleveren zouden op grote schaal te exploiteren zijn met datamining tools.[76]

De informatiepotentie van cyber-identiteiten binnen open en niet-openbare bronnen is enorm en versterkt langs digitale weg de inlichtingencapaciteit (thuis en in operatiegebieden).

● *'Soft cyber': passieve inzet van cyber-identiteiten*
Via social media en internet kunnen cyber-identiteiten (van medestanders, neutralen en zelfs tegenstanders) passief worden benaderd met als doel informatie te verspreiden of een dialoog te voeren. Dit loopt via eigen cyber-identiteiten: via accounts die gelieerd zijn aan de overheid, krijgsmacht, politici of militairen.[77] Zie de profielen en accounts van de minister (zie figuur 6) en krijgsmacht (onder-)delen op bijvoorbeeld Facebook, Linkedin en Hyves, foto- en videohosting internetservices (zoals YouTube en Flickr),[78] Wikipedia-pagina's[79] en blogs (bijvoorbeeld *Tumblr* en *Wordpress*).[80]

Het beoogde effect is bijvoorbeeld het vergroten van het draagvlak voor de krijgsmacht en haar missies, wat de eigen mentale component ten goede komt.[81] Een illustratie is de tweet van Peter van Maurik, *geretweet* door KTZ Rob Hunnego, samen goed voor duizend volgers (zie figuur 11).

Dit typeren we als een vorm van 'soft cyber': het effect is niet-fysiek, de operatie loopt via cyberspace met internet als vector. De inzetmiddelen (eigen cyber-capaciteit) én het adressaat zijn cyber-identiteiten, waarmee indirect mensen beïnvloed kunnen worden. 'Soft cyber' is daarmee ook een specifiek middel in informatieoperaties.

● *'Soft cyber' in operatiegebieden*
Passieve soft cyber wordt ook in operatiegebieden toegepast.[82] De werking is vergelijk-

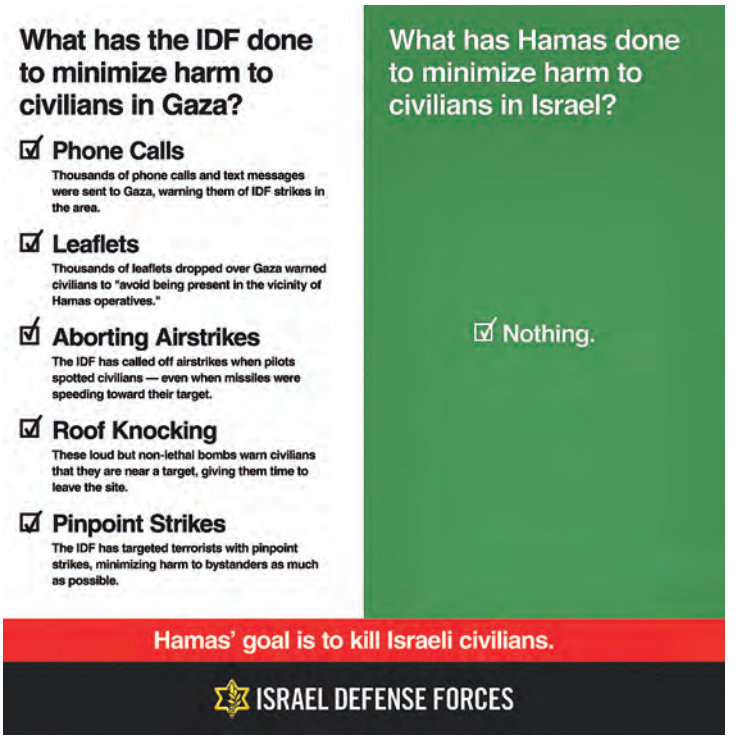
73 Pfleeger & Pfleeger (2007) 404-414.
74 Andress & Winterfeld (2011) 140-141.
75 Andress & Winterfeld (2011) 140-141.
76 Andress & Winterfeld (2011) 144.
77 Zie ook <defensie.nl/actueel/social_media>.
78 Youtube.com/user/defensie.
79 Wikipedia.org/wiki/Koninklijke_Landmacht.
80 US DoD, Directive-Type Memorandum (DTM) 09-026 (2010, Feb) *Responsible and Effective Use of Internet-based Capabilities*,5 , via: www.carlisle.army.mil/DIME/documents/DODNewMediaPolicyFeb10.pdf.
81 Zie de oproep 'soft cyber': 'Cyber en militair vermogen', in: *Militaire Spectator* 181 ((2012) (12).
82 Zie: J. van der Meulen & R. Moelker, 'Digital Duels in the Global Public Sphere. Social Media in Civil Society and Military Operations', in: Ducheine, Osinga & Soeters (2012). *Cyber warfare: critical perspectives*, 141.

baar met hetgeen hiervoor is beschreven, maar dan gericht op tegenstanders, medestanders of neutralen in het buitenland. Bekende voorbeelden zijn de 'verbale' twitterduels uit de Tweede Gazaoorlog tussen *@IDFSpokesperson* (216.112 volgers) en Hamas. Volgers van de *@IDFSpokesperson* en Facebook-vrienden ontvangen deze afbeelding (zie figuur 12)[83].
Nederlands zet vooralsnog slechts beperkt cyber-identiteiten in uitzendgebieden in en concentreert zich daarbij op het thuisfront.[84]
Voor zover 'operationele veiligheid' of OPSEC een reden voor terughoudendheid is,[85] kan deze geborgd worden door gebruikers goed te instrueren.[86] Indien (nog steeds) wordt gedacht dat de bevolking in potentiële operatiegebieden geen toegang heeft tot social media of andere media, wordt dit door huidige ontwikkelingen tegengesproken.

Vooral in het Midden-Oosten (2640 procent toename tussen 2000-2012), Afrika (3607 procent)[87] en Azië (860 procent) groeit mobiel internet sterk.[88] De rol van social media in de Arabische Lente is een mooi voorbeeld van deze ontwikkeling.[89]
De inzet van cyber-identiteiten tijdens operaties kan samenvallen met (het doel van andere) informatieoperaties, *Strategic Communication* en bijvoorbeeld *key leader engagement*.
Het lijkt een veelbelovende maar relatief onontgonnen capaciteit. Key leader engagement kan ook langs deze digitale weg vorm krijgen (zie hierna).

● *Actieve beïnvloeding van cyber-identiteiten*
Cyber-identiteiten kunnen (ook) gericht en actief worden benaderd om indirect andere personen of groepen te beïnvloeden. Op basis van bijvoorbeeld sentiment of achtergrond, te achterhalen met datamining tools, en met herleide gebruikersgegevens (cyber-identiteiten) is interactie met individuen of groepen mogelijk.

Persoonlijke interactie is daarbij effectiever dan generieke communicatie, maar uiteraard ook arbeidsintensiever. Efficiënter én effectiever is het aanspreken van sleutelfiguren die ook weer via datamining bepaald kunnen worden.[90]
Deze werkwijze heeft overeenkomsten met



Figuur 12. IDF-bericht
(Tweet van @IDFSpokesman en IDFBlog.com)

key-leader engagement binnen klassieke informatieoperaties.[91]
Een bijzondere vorm van disruptieve beïnvloeding is het toebrengen van imagoschade aan key leaders. De geloofwaardigheid of reputatie van vooraanstaande personen kan via cyber-identiteiten op effectieve wijze worden aangetast, met eventuele 'uitschakeling' van de persoon als gevolg.

83 Tweet @IDFSpokesman (en IDFBlog.com) tijdens Tweede Gazaoorlog (Operatie *Pillars of Defence*), via: <www.idfblog.com/wp-content/uploads/2012/11/checklistinfographic.jpg>.
84 Zie: <defensie.nl/missies/actueel/algemeen/2013/03/12/46203777/Weekoverzicht_Defensie_operaties_video>.
85 Voor overwegingen omtrent OPSEC zie: K.C. Dreijer (2010) *Social Media: Friendly Fire op het Internet?* Bachelorscriptie NLDA, via: <defbib.kma.nl/art2/pdf/ada/Dreijer%20K.C.pdf>.
86 Zie ook *US Army Social Media Handbook* (2012), Optimizing Online Engagement, 2 , via: < armylive.dodlive.mil/index.php/2011/01/u-s-army-social-media-handbook-is-here/>.
87 Zie *NRC Handelsblad*,18 juni 2013, Afrika springt het digitale tijdperk in.
88 *Internet Usage Statistics: The Internet Big Picture*, via: <internetworldstats.com/stats.htm>.
89 Zie: <syriatracker.crowdmap.com>.
90 Zie: <newsroom.edelmanpr.nl/jeanine-hennis-plasschaert-meest-invloedrijke-kabinetslid-op-twitter/>.
91 LDP I,140. Zie: M. Kitzen, S. Rietjens, F. Osinga, 'Learning soft power the hard way, military adaptation by the Netherlands' Task Force Uruzgan, in: T. Farrell, F. Osinga & J. Russell (Eds.), *Military Adaptation in Afghanistan* (Stanford University Press, 2013).

● *Cyber-identiteiten manipuleren of vernietigen*
Indien cyber-identiteiten toegankelijk zijn, bijvoorbeeld doordat een wachtwoord via social engineering verkregen is, kan het gemanipuleerd, gemuteerd, ontoegankelijk gemaakt of vernietigd worden.

Exploitatie van cyber-objecten
Steeds meer (en steeds vaker) worden fysieke objecten op internet aangesloten om snelle informatieoverdracht te faciliteren en gebruikersgemak te vergroten.[92] Voorbeelden zijn: auto's, printers, huishoudelijke elektronica en zelfs pacemakers en insulinepompen.[93] Deze fysieke objecten hebben een digitale representatie in het cyber-domein, het cyber-object.
Analoog aan het beïnvloeden van fysieke personen (en hun psyche) via cyber-identiteiten, kunnen fysieke objecten worden gemanipuleerd via hun virtuele afspiegeling: cyber-objecten.
Deze optie is bij uitstek geschikt om het digitale vermogen van de krijgsmacht te vergroten.

● *Inzet fysieke objecten*
Een cyber-operatie zou kunnen bestaan uit het aanbieden van infrastructuur. Bijvoorbeeld in de vorm van een internetcafé, (mobiele) gsm-mast, routers, servers, (WIFI-)netwerk.
Op deze manier kan informatie worden verzameld over de gebruikers van deze fysieke (en digitale) objecten.[94] Zo zou ook een internetserviceprovider kunnen worden opgericht, of een IT-beveiligingsbedrijf waarmee cyber-objecten en cyber-identiteiten (van klanten) benaderbaar worden.

● *Monitoren cyber-objecten*
Via (eigen) cyber-identiteiten kan online informatie worden verzameld over een aan te grijpen of te beïnvloeden cyber-object.
Dit kan ongemerkt en zonder direct contact te maken met het cyber-object via open bronnen zoals databases (e.g. *Shodan HQ*),[95] handleidingen en websites met informatie over het cyber-object.

Een alternatief is het actief monitoren met specifieke software (een eigen cyber-object) die het cyber-object in kaart brengt. Deze software (bijvoorbeeld *Nmap* of *Metagoofil*)[96] verzamelt informatie over de zwakheden, architectuur, locatie en een variëteit aan andere bruikbare informatie.[97] Deze informatie kan inzicht bieden over het functioneren, beheer, locatie en kwetsbaarheden van het cyber-object en het gekoppelde fysieke object.

● *Externe manipulatie cyber-objecten*
Cyber-objecten kunnen ook worden gemanipuleerd. De meest basale vorm is van buitenaf, zonder toegang te forceren. Met een zogeheten (*distributed*) *denial of service* of (D)DOS-aanval wordt het cyber-object, bijvoorbeeld een digitale dienst als DigiD, overladen met dataverkeer waardoor deze tijdelijk onbereikbaar is.[98]
Om een (D)DOS aanval uit te kunnen voeren is een eigen (of overgenomen) bot-netwerk[99] nodig[100] of worden sympathisanten gemobiliseerd.[101] Daarnaast bestaan ettelijke methoden om cyber-objecten te manipuleren.[102] De technische beschrijving van de modus operandi van dit soort aanvallen valt te ver buiten de doelstelling van deze bijdrage.

92 Ook wel het '*Web of objects*' of '*the Internet of Things*' genaamd.
93 Daily Mail online (10 april 2012), *Hackers 'can gain access to medical implants and endanger patients' lives'*. <http://www.dailymail.co.uk/health/article-2127568/Hackers-gain-access-medical-implants-endanger-patients-lives.html>.
94 Zoals ten tijde van de G20-top in London (2009), zie *NRC Handelsblad*, 17 juni 2013, *Britse geheime dienst luisterde G20 in Londen af*.
95 *Shodan* is een zoekmachine die een gebruiker in staat stelt om specifieke systemen en computers te vinden en bekende data te raadplegen aangaande het systeem, in tegenstelling tot de Google zoekmachine die informatie vindt.
96 *Nmap* stelt gebruikers in staat om cyber-objecten te scannen op – onder meere – open (toegangs-)poorten, kwetsbaarheden en besturingssysteem. *Metagoofil* zoekt naar metadata (data met gegevens over data). Uit deze metadata kan bijvoorbeeld worden opgemaakt wie de data heeft aangemaakt en aangepast; waar de data opgeslagen is geweest; welke wijzigingen in tekst of data er zijn gemaakt, de locatie waar een foto is gemaakt en met welk toestel, e.d..
97 Andress & Winterfeld (2011) 88-100.
98 Zoals onlangs (waarschijnlijk) het geval was bij DigiD en iDeal: zie NCSC, 9-4-2013, *DDOS-aanval zorgde voor verstoring bereikbaarheid websites*, zie: <www.ncsc.nl/actueel/nieuwsberichten/ddos-aanval-zorgde-voor-verstoring-bereikbaarheid-websites.html>.
99 Een bot-netwerk bestaat uit gekoppelde gecompromitteerde (gehackte) systemen die ter beschikking staan van een cyber-operator om te gebruiken in een variëteit aan cyber-operaties, waaronder een DDOS.
100 Zie NCSC, 15-5-2013, *Factsheet Continuiteit van online diensten*, <www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets>.
101 Zoals Anonymous dit toepast. Zie <resources.infosecinstitute.com/loic-dos-attacking-tool>.
102 Bijvoorbeeld via *domain name servers* (DNS), routers en lokale *host* files: Pfleeger & Pfleeger (2007) 422, 429-432. Ook door inbedding in hardware, operating systems, veranderingen in programmatuur en de updates daarvan, *spoofing* van IMEI- en MAC-adressen, e.d.

● *Intrusie voor interne manipulatie*
Cyber-objecten zijn van binnenuit beter te manipuleren, hetgeen toegang vereist.[103] Intrusie valt op diverse manieren te realiseren. Eenvoudige wachtwoorden kunnen worden gekraakt met software als *Hydra* en *John the Ripper*,[104] of via social engineering (phishing of pharming) en eerder gecompromitteerde wachtwoord-databases[105] herleid worden.[106]

Toegang kan ook worden gerealiseerd door (bekende en onbekende) kwetsbaarheden (de zogeheten *exploits*) van een cyber-object te benutten. Bekende exploits van veelgebruikte besturingssystemen en databases zijn online beschikbaar.[107] Bovendien bestaat er software zoals *Metasploit en Immunity CANVAS*[108] om deze exploits effectief te benutten.[109] Sommige bedrijven specialiseren zich in nog onbekende kwetsbaarheden (*zero-days*) en verkopen deze aan de hoogste bieder.[110]

Na intrusie kan de toegang tot het cyber-object worden bestendigd en uitgebreid door bepaalde *payloads* uit te voeren op het systeem.[111] Denk aan het openen van een digitale poort van het fysieke of cyber-object,[112] het installeren van een (*reverse*) *shell*,[113] toevoegen van geautoriseerde gebruikers (bijvoorbeeld administrators) en het creëren van *backdoors*.[114] Zo ontstaan meer mogelijkheden (bevoegdheden en bewegingsruimte) binnen het cyber-object en wordt toekomstige toegang gewaarborgd. Op deze manier kunnen ook de intrusie, actie en manipulatie worden 'gecamoufleerd' (zie figuur 8).

● *Interne manipulatie*
Vervolgens kan het cyber-object door de indringer worden gemanipuleerd. Manipulatie kan onder meer bestaan uit het veranderen van de instellingen, het beheer, het functioneren en het gebruik van het cyber-object (en het gekoppelde fysieke object). Het cyber-object wordt dan door anderen gecontroleerd en beheerst.

Zo kunnen ondersteuningssystemen voor commandovoering worden verstoord, kan desinformatie worden verspreid, toegang worden ontzegd, informatie worden gemuteerd of onttrokken.[115]

Indien het cyber-object is gekoppeld aan een computer kan deze als extra computervermogen voor basale taken worden ingezet. Bijvoorbeeld het verspreiden van berichten (*spam*) en software, het kraken van wachtwoorden of voor (D)DOS aanvallen. Daarnaast is de gecompromitteerde computer beschikbaar als aanvalsvector bij toekomstige cyber-operaties. Zodoende zijn cyber-aanvallen te lanceren vanaf de gecompromitteerde computer en niet vanaf eigen systemen, hetgeen misleiding en verrassing ten goede komt en de herkomst camoufleert.

Indien het overgenomen cyber-object een besturingssysteem van fysieke objecten betreft, kunnen deze fysieke objecten worden gemanipuleerd. De inzet van Stuxnet tegen het

103 Via het besturingssysteem of de database van het doel. In het geval van SQL injectie (SQLi) is het discutabel of toegang tot een systeem daadwerkelijk een premisse is om een systeem te manipuleren.
104 *Hydra* kan worden gebruikt om een groot aantal veelgebruikte of waarschijnlijke wachtwoorden en gebruikersnamen uit te proberen. *John the Ripper* kan worden gebruikt om wachtwoord *hashes* (versleutelde wachtwoorden) in te voeren en uit te proberen.
105 Zie: <pastebin.com/XvbzgW64>.
106 Andress & Winterfeld (2011) 100-101.
107 Zie bijvoorbeeld voor Windows XP: <www.exploit-db.com/platform/?p=windows>.
108 *Metasploit* kan gebruikt worden om (1) systemen te scannen, (2) een *exploit* te selecteren voor het gescande systeem, (3) deze te voorzien van een *payload* en (4) de *exploit* met *payload* uit te voeren op het doelsysteem. *Immunity CANVAS* kan worden gebruikt om (semi-)automatisch toegang te krijgen tot doelsystemen en deze vervolgens te exploiteren via een scala aan *exploits* en *payloads*.
109 Andress & Winterfeld (2011)103-105.
110 Het Franse Vupen is een bedrijf dat *zero-days* verkoopt aan voornamelijk overheden en bedrijven: A. Greenberg, in: *Forbes.com* (23 maart 2012), 'Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits', via <forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>; J.M. Schwartz, *Blackhole Botnet Creator Buys up Zero Day Exploits*, in: <www.informationweek.com/security/vulnerabilities/blackhole-botnet-creator-buys-up-zero-da/240145769>.
111 Andress & Winterfeld (2011) 109.
112 Computers, netwerken en andere systemen maken gebruik van 'poorten' om onderling te communiceren. Zo kan een poort dicht zijn of gebruikt worden om te luisteren of zenden. Poort 80 op een pc wordt (standaard) bijvoorbeeld gebruikt voor *Hypertext Transfer Protocol* (http), oftewel het surfen op het internet.
113 *Reverse shells* zorgen ervoor dat een doel-systeem verbinding zoekt met het systeem van de hacker. *Shells* in het algemeen zorgen ervoor dat de *operator* bepaalde opdrachten kan in- en uitvoeren op het doel-systeem.
114 *Backdoors* zorgen ervoor dat een hacker een alternatieve toegang heeft tot het systeem, die niet geblokkeerd wordt door beveiligingsupdates in software.
115 *Deception, disruption, denial, degradation, & destruction* (5 D's), in de duiding van Andress & Winterfeld, (2011) 110.

Adressaat	*Cyber-identiteit*	*Cyber-object*
Effect		
Constructief	Info verzamelen • Datamining • Social engineering (o.a. Phishing, Pharming) Info verspreiden • Passieve soft-cyber Interactie Beïnvloeden • Actieve soft-cyber, o.a. key leader engagement	Scannen Info verzamelen Exploits ontwerpen tbv intrusie
Disruptief	Beïnvloeden / misleiden Irrelevant maken Manipulatie Blokkeren Vernietigen	Extern manipuleren • Kraken • Overbelasten Intrusie Intern Manipuleren • Camoufleren • Upgraden • Disfunctioneren • Misbruiken (bot of vector) • Blokkeren Vernietiging

Tabel 1: Cyber-activiteiten

Iraanse atoomprogramma door het aanpassen van de besturing van de centrifuges voor uraniumverrijking is hier een voorbeeld van.[116]

• *Vernietigen cyber-objecten (offensieve actie)*
Na manipulatie functioneert het cyber-object nog wel, maar op een andere manier. Vernietiging leidt tot disfunctioneren van het cyber-object, bijvoorbeeld door het wissen van data of besturingssystemen. Vernietiging is alleen compleet indien er geen back-up beschikbaar is. Met een *back-up* zal 'slechts' sprake zijn van een tijdelijke onderbreking van de functionaliteit van het cyber-object.[117]

Toegang tot het cyber-object en beheerprivileges zijn een vereiste voor digitale vernietiging (i.e. wissen); deze kunnen via de eerder genoemde methoden worden gerealiseerd.

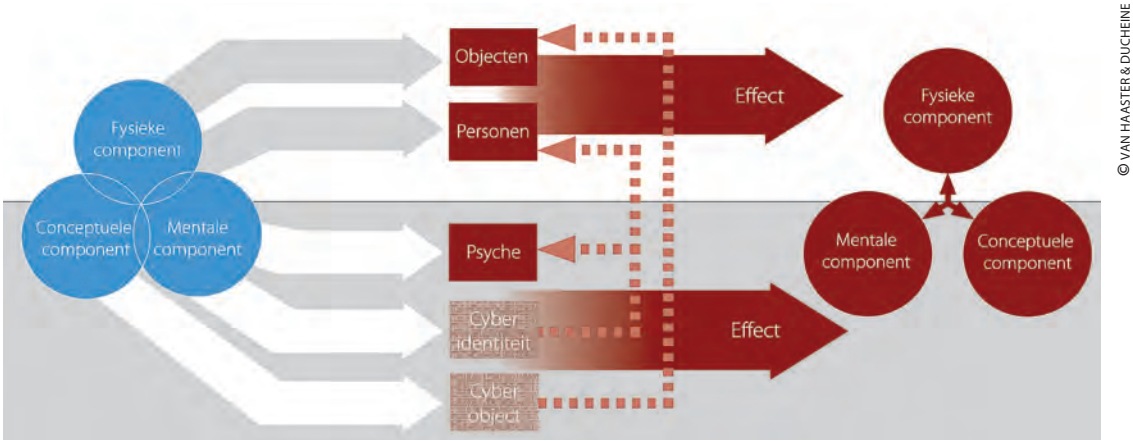
Effecten
Cyber-operaties zijn volgens de NDD een variant van informatieoperaties.[118] Deze laatste beogen niet-fysieke effecten: het beïnvloeden van tegenstanders, medestanders en neutralen. Met cyber-operaties kunnen volgens onze analyse zowel (directe en indirecte) niet-fysieke als indirecte fysieke effecten worden bereikt.[119] De effecten van cyber-operaties worden primair bepaald door de (deel)doelstelling (zie figuur 8) van die operatie. In een verkennende fase is het beoogde effect 'beperkter' dan in de actie-fase, waarin een vergaand effect, bijvoorbeeld tijdelijke of permanente onbereikbaarheid, controle of zelfs destructie beoogd kan zijn. De effecten variëren van constructief tot disruptief.

116 D. Sanger, *Confront & Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown, New York, 2012).

117 *Wiper malware*, ontdekt op Iraanse systemen, is specifiek ontworpen is om snel data te vernietigen. Zie K. Zetter, K. (28 mei 2012), *Meet 'Flame', The Massive Spy Malware Infiltrating Iranian Computers*, via <wired.com/threatlevel/2012/05/flame/>.

118 NDD (2013) 99.

119 Zoals bijvoorbeeld Stuxnet.



Figuur 13. Militair vermogen en (cyber-)operaties

De effecten hangen uiteraard ook samen met het adressaat van de operatie. Manipulatie van cyber-objecten kan directe disruptieve gevolgen voor het cyber-object hebben, maar ook indirecte fysieke gevolgen voor het gekoppelde fysieke object. Manipulatie van cyber-identiteiten zal minder snel fysieke consequenties hebben. Maar gemanipuleerde cyber-identiteiten kunnen imagoschade creëren, waarmee personen 'irrelevant' te maken zijn. Uiteraard worden de effecten ook bepaald door de doelgroepen: tegenstanders, medestanders en neutralen. Disruptieve effecten bij medestanders zijn moeilijk voorstelbaar.
Het spreekt voor zich dat deze in cyber te realiseren effecten moeten bijdragen aan de politiek-strategische doelstelling waarvoor militair vermogen wordt ingezet. Met andere woorden, de ultieme effecten zullen moeten bijdragen aan strategisch te realiseren effecten waarvoor de krijgsmacht wordt ingezet.

Conclusie

Onze doelstelling was de plaats van cyber-operaties binnen militair vermogen te bepalen en te bezien hoe de krijgsmacht cyber-operaties (en cyber warfare) doctrinair kan operationaliseren. Uit onze analyse blijkt dat cyber-operaties – via een interpretatie van de niet-fysieke elementen – in gangbare modellen van militair vermogen passen. Ze zijn instrumenteel in het realiseren van strategische doelstellingen door het beïnvloeden van (het vermogen van) andere actoren. Cyber-operaties vinden plaats in of via het digitale domein, bestaande uit een fysieke en een niet-fysieke dimensie. De niet-fysieke dimensie van cyberspace, de virtuele laag (logical layer), maakt cyber-operaties bijzonder ten opzicht van operaties in het fysieke domein (en een aantal andere informatieoperaties). Deze virtuele laag bevat unieke capaciteiten, cyber-identiteiten en cyber-objecen, die om te zetten zijn in capabilities en daardoor bijdragen aan het totale eigen (militaire) vermogen. Cyber-operaties genereren effecten door zich te richten op de cyber-capaciteiten en capabilities in het (militaire) vermogen van andere actoren. Het adressaat van cyber-operaties bestaat uit de cyber-identiteiten en cyber-objecten in dat vermogen van anderen. De effecten zelf variëren van constructief tot disruptief en zijn veelal indirect ten opzichte van adressaten in de fysieke dimensie.

Twee misverstanden willen we aanstippen. Cyber warfare is meer dan 'het aanvallen van een hacker' of het 'targeten van een server', zoals regelmatig wordt gehoord. Een ander is de relatie tussen cyber-operaties en informatie-operaties. Cyber-operaties volgen qua principe informatieoperaties, maar qua adressaat nemen ze een unieke positie in. Ook 'soft cyber' operaties zijn daardoor afwijkend ten opzicht van gangbare informatieoperaties.

We willen verder volstaan met een integraal schema waarin de verschillende onderdelen van cyber een plaats krijgen binnen militair vermogen en dat bovendien een model voor cyber-operaties naast reguliere operaties in de andere domeinen representeert. Voor de overzichtelijkheid hebben we de doelgroepen medestanders en neutralen in dit schema niet gedetailleerd opgenomen. ■

Storytelling: a lifesaving tool?

Verhalen als bron voor veilig optreden in extreme omstandigheden

Vooral in het domein van hoog-risico activiteiten, zoals bij Defensie en de brandweer, kan *storytelling* van grote waarde zijn. Storytelling is geen *managementtool* dat een gegarandeerde empirische uitkomst kent, maar niettemin kan het het 'collectieve geheugen' van een organisatie dienen. Storytelling wordt binnen Defensie al toegepast, maar veelal onbewust. Een meer bewust gebruik zou bij kunnen dragen aan het creëren van een zo veilig mogelijke werkomgeving onder risicovolle omstandigheden. Een methodiek van storytelling die de Brandweer Flevoland heeft ontwikkeld lijkt een veelbelovend instrument om aan het arsenaal van het Veiligheidsmanagementsysteem Defensie toe te voegen. Een mogelijkheid is het uitvoeren van een *pilot* storytelling in nauwe samenwerking met de brandweerorganisatie, waarbij ervaringen van beide organisaties naast elkaar worden gelegd onder gelijktijdige uitwisseling van overige kennis en ervaring.

*G.C.H. Bakx, MSc, J.F. van Opstal MCM en dr. T. Bijlsma**

In het kader van zijn masterstudie voerde Jeroen van Opstal, kennisregisseur en hoofdofficier van dienst bij de Brandweer Flevoland, een onderzoek uit naar het fenomeen *storytelling* bij de brandweer. Meer in het bijzonder richtte hij zich hierbij op storytelling in organisaties, ofwel het in verhaalvorm gieten en verspreiden van organisatorische, maar persoonlijke belevenissen die in een hoog-risico omgeving zoals de brandweer veelal worden opgedaan. Zo is het, volgens de literatuur althans, mogelijk om doelgericht en op een natuurlijke wijze te bouwen aan consensus en aan een cultuur van gedeelde inzichten en waarden binnen de eigen organisatie.[1]

Van Opstal interviewde negentig leidinggevenden binnen Brandweer Flevoland, voerde veldonderzoek uit en verzorgde workshops voor operationeel leidinggevenden.
Het onderzoek leidde uiteindelijk tot een werkbaar concept om informele leerverhalen in organisaties te 'vangen' en te 'regisseren', met als doel het lerend vermogen en het bewustzijn van die organisaties te vergroten. De brandweer en defensie zijn tot op zekere hoogte vergelijkbare organisaties. Van Opstals onderzoek was dan ook de aan-leiding voor het schrijven van dit artikel, dat een koppeling maakt tussen storytelling en de defensieorganisatie.

Grootschalige ongevallen kunnen onze gangbare risicomodellen (onze ideeën hoe de wereld in elkaar zit) volledig op hun kop zetten. Veelal is het hierdoor dat betrokkenen in opperste verwarring achterblijven. Het vertellen van verhalen is een manier om dit risicomodel te repareren, of – liever gezegd – te actualiseren: hier zijn we dus kwetsbaar. Leerprocessen zijn bij Defensie veelal formeel en expliciet vorm-

* Majoor KLu Gwendolyn Bakx is universitair docent Human Factors en Systeemveiligheid bij de capaciteitsgroep Militaire Bedrijfswetenschappen van de Faculteit Militaire Wetenschappen, Nederlandse Defensie Academie in Breda. Zij is tevens coördinator Research en Expertise Centrum Human Factors and System Safety van de NLDA; Commandeur (Brw) Jeroen van Opstal is kennisregisseur en hoofdofficier van dienst bij Brandweer Flevoland; Tom Bijlsma is universitair docent bij de capaciteitsgroep Militaire Bedrijfswetenschappen van de Faculteit Militaire Wetenschappen, NLDA.

1 R. Delgado, 'Storytelling for oppositions and others. A plea for narratives' in: *Michigan Law Review* (1989) (84) 2412.

gegeven in cursussen, trainingen, oefeningen en evaluaties. Storytelling, daarentegen, draait om een meer informele en impliciete vorm van leren waarbij de boodschap – attractief en persoonlijk verpakt – vaak beter beklijft. Vooral in organisaties die werken in een dynamische omgeving met hoog-risico processen lijkt storytelling een belangrijke rol te kunnen spelen. Er gebeurt vaak veel in dit soort organisaties, waardoor de kans bestaat dat de lessen van gisteren worden overschaduwd door die van vandaag, vooral als wanneer iemand ze in rapportagevorm moet lezen. Informelere en tot de verbeelding sprekende methodieken kunnen dan uitkomst bieden.
Verhalen dienen om ervaringen uit te wisselen, maar vormen ook, indien meer geïnstitutionaliseerd toegepast, een manier om het 'collectieve geheugen' te voeden. Verhalen zijn namelijk bijzonder krachtig. Vroeger waren mensen zelfs op verhalen aangewezen, niet alleen voor vermaak, maar juist ook voor de overdracht van 'overlevingskennis' en cultuuruitingen. Onze mythen, sagen, fabels en sprookjes zijn op die manier ontstaan. Ook kiezen we vaak leiders met een goed verhaal.[2] Over het gebruik van verhalen als gerichte leerinterventie is binnen Defensie echter nog weinig geschreven. Met dit artikel proberen we daar meer invulling aan te geven. We beschouwen storytelling daarbij vanuit de optiek van veiligheid. Allereerst beschrijven we enkele kenmerken van storytelling die het fenomeen zo geschikt maken als bijzondere leerstrategie en de voor- en nadelen ervan. Vervolgens kijken we hoe storytelling een actief in te zetten leerinterventietechniek kan zijn. Aansluitend gaan we in op de huidige situatie op dit terrein binnen Defensie, om vervolgens een methodiek voor te stellen om storytelling in te zetten binnen hoog-risico organisaties zoals Defensie.

Storytelling als socialisatievorm

Een noodzakelijke leervorm voor organisaties is 'socialisatie',[3,4] het uitwisselen of 'toetsen' van ervaring(en) binnen de eigen groep, de eigen organisatie, of het eigen organisatieonderdeel. Het gaat hierbij om het delen van een bepaalde vorm van kennis, de zogeheten

FOTO AVDD, A. RORIMPANDEY

Bij Defensie kan storytelling bijdragen aan het creëren van een zo veilig mogelijke werkomgeving onder risicovolle omstandigheden

tacit knowledge, zonder deze expliciet onder woorden te brengen. Deze leervorm komt vaak terug in meester-gezel relaties, waarin de leerling de gewenste werkwijze van zijn of haar praktijkbegeleider meer impliciet dan expliciet krijgt aangereikt. Socialisatie is een bekende leervorm binnen Defensie. Door de jaren heen leren we zo de 'onbeschreven' kneepjes van het vak.
Een bijzondere vorm van dit socialiseren is het vertellen van verhalen waarbij ervaring(en) worden 'verpakt'. Van belang daarbij is de narrativiteit: datgene dat losse gebeurtenissen tot een coherent geheel maakt.[5] Zaken die soms ogenschijnlijk niets met elkaar van doen lijken te hebben, worden door de verhaallijn onbewust en intuïtief aan elkaar gekoppeld. Narrativiteit geeft daarmee structuur aan wat anders niets meer dan een continue brei aan gebeurtenissen lijkt te zijn.[6] Een belangrijke functie van een verhaal is dan ook de natuurlijke koppeling van (aspecten van) gebeurtenissen door de betekenis die verteller en toehoorders daaraan toekennen. Weick noemt dit treffend *sensemaking*.[7] Verhalen geven hierdoor een betekenis aan de dagelijkse

2 A. Schutte en T. Hendriks, *Corporate Stories. Verwoorden, vertellen en verankeren* (Amsterdam, Kluwer, 2007) 52, 110.
3 E.H. Schein, 'Organizational socialization and the profession of management' in: *Industrial Management Review* (1968) (9) 3.
4 I. Nonaka en H. Takeuchi, *De Kenniscreërende Onderneming. Hoe Japanse bedrijven innovatieprocessen in gang zetten* (Schiedam, Scriptum Management, 1997).
5 B. Czarniawska, *Writing management. Organization theory as a literary genre* (Oxford, Oxford University Press, 1999) 2.
6 K.E. Weick, *Sensemaking in Organizations* (Thousand Oaks, Sage Publications, 1995) 184.
7 Idem, 184.

realiteit; een realiteit van persoonlijke levens- en leerervaringen en soms van omgaan met leven en dood.
Storytelling maakt het mogelijk om impliciet – en aantrekkelijk verpakt – 'kennis' met anderen te delen. Hier ligt dan ook de grote winst. Net als bij de verhalen van vroeger gaat het om de overdracht van de onderliggende 'levenslessen'. Zo zorgt storytelling ook voor een informele, maar krachtige kennisoverdracht. De narrativiteit geeft een verhaal kracht en authenticiteit. Bovenal zit de kracht echter in de eenvoud waarmee een verhaal in het geheugen achterblijft en door te vertellen is. Men moet het verhaal van de ander zelf kunnen zien, kunnen proeven en zelfs kunnen voelen.
Om het uiteindelijke leereffect te kunnen bewerkstelligen zal de toehoorder bovendien, geïnitieerd en gestimuleerd door de verteller, zijn of haar eigen verhaal op moeten kunnen bouwen.
Het is dan ook van belang dat de toehoorder zich kan vereenzelvigen met de verteller. Naast het overbrengen van oprechte emotie spelen daarbij de mechanismen identificatie en associatie een rol.[8] Emoties, empathie en verbondenheid zorgen er voor dat de benodigde uitwisseling van mentale modellen plaatsvindt, evenals de projectie naar vergelijkbare situaties. Doordat storytelling op het gevoels- en betrekkings-niveau speelt, ontstaat soms zelfs een nog veel verdergaande projectie, bijvoorbeeld naar situaties die op het oog wezenlijk anders zijn, maar onder de oppervlakte blijkbaar wel degelijk vergelijkbare elementen in zich hebben.

De voordelen van impliciet en informeel

Niet alles wat in een organisatie wordt verteld valt onder storytelling. Hatch maakt in dit verband onderscheid tussen de overdracht van (expliciete) analytische kennis door bijvoorbeeld gestructureerde lesprogramma's en de overdracht van (impliciete) in de praktijk opgedane kennis door het vertellen van verhalen.[9] Terwijl de analytische kennis geworteld is in een mechanistisch wereldbeeld waarin gebeurtenissen, mensen en middelen bijna sturend voorspelbaar zijn, zijn verhalen juist bedoeld om meer inzicht te verlenen in de context waarin gebeurtenissen plaatsvinden. Verhalen over bedrijfsongevallen en bijna-ongevallen of *critical incidents* kunnen bijvoorbeeld voor professionals zeer betekenisvol zijn. Soms zelfs vormen ze een sleutel naar de toekomst. Hiervoor zijn meerdere redenen aan te dragen. Zo geeft storytelling door het min of meer informele karakter ervan ruimte om te praten over wat er is gebeurd en over welke betekenis het voor de verteller heeft. Dat creëert een sfeer die een meer open communicatie mogelijk maakt. Het haalt bovendien de aandacht weg van wie of wat er gefaald zou hebben. Idealiter leidt storytelling er zelfs toe dat anderen zich uitgenodigd voelen hetzelfde te doen: hun verhaal vertellen, om aan te vullen, om een andere visie te geven, om verhalen samen te voegen of wat dan ook. Juist na incidenten en ongevallen kan storytelling dan ook van een aanzienlijke meerwaarde zijn.

De crux van een verhaal maakt deel uit van de beleving van mensen. Verhalen van vakgenoten kunnen hierdoor de eigen ervaring gemakkelijker voeden. Dit kan van cruciaal belang zijn, vooral voor toekomstige tijd-kritische intuïtieve besluitvorming.[10] De kwaliteit van deze vorm van besluitvorming lijkt namelijk af te hangen van een vlotte beschikbaarheid van analogieën. Door het delen van ervaringen lijkt men dan ook beter in staat om bij toekomstige voor-vallen anders – lees: hoewel nog steeds intuïtief, toch bewuster – te reageren. Storytelling draagt daarom bij aan daadwerkelijke bewustwording en gedragsverandering en kan in die zin soms meer teweegbrengen dan dikke evaluatierapporten vol met abstracte begrippen en leerprincipes.[11] Kortom, storytelling kan als leerinterventie weleens van cruciaal belang zijn bij kennismanagement binnen hoog-risico activiteiten.

8 F. Breuer, 'Storytelling als interactieve interventie', in: J.J. Boonstra & L.C.A. de Caluwé, *Interveniëren en Veranderen. Zoeken naar Betekenis in Interacties* (Deventer, Kluwer, 2006) 64.

9 T. Hatch, *Into the Classroom. Developing the Scholarship of Teaching and Learning* (Indianapolis, Jossey-Bass, 2005).

10 G. Klein, *Sources of Power*. How People Make Decisions (Cambridge, MIT Press, 1998) 21.

11 E. Oomes, 'De Vanzelfsprekendheid van Alledag. Een beschouwing in drie delen over de gewoonten in het brandweervak', *Lectorale rede*, 15 september 2006 (Nederlands Instituut Fysieke Veiligheid [NIFV] / Nederlandse Vereniging voor Brandweerzorg en Rampenbestrijding [NVBR], 2006).

Is storytelling dan per definitie zaligmakend?

Stickiness

Verhalen hebben een hoge 'relatieve waarde'. Dat betekent dat de waarde van de impliciete kennis die in het verhaal verpakt zit onvermijdelijk een subjectieve weergave van de werkelijkheid is. Het zijn immers geen objectieve constanten die worden gedeeld in verhalen. Eerder zijn het de finesses zoals die van het vakmanschap, van kennis van de informele organisatie, werkende *workarounds* en van inschattingen en analyses die professionals vaak maken op basis van hun (geïnformeerde) intuïtie. Ook analyses op basis van het zogeheten 'niet-pluis-gevoel' vinden hun basis eerder in storytelling dan in officiële rapporten. De term 'niet-pluis-gevoel' is afkomstig uit de medische sector en staat voor een soort onderbuikgevoel van professionals met een bewezen waarde: de professional heeft het gevoel dat er iets niet in de haak is, maar kan nog niet volledig de vinger achter het waarom krijgen.[12]

Een reden voor die relatieve waarde is dat verhalen organisch ontstaan in de zin dat ze op spontane wijze ontkiemen. In eerste instantie bestaan ze daarna als een nog niet volgroeide vertelling, waarvan de reikwijdte bovendien veelal initieel beperkt blijft tot de eigen gemeenschap.[13] Storytelling betreft in eerste instantie dan ook informele gemeenschappen waaraan mensen een groepsidentiteit ontlenen.[14] Hierdoor verspreidt kennis onder vakbroeders zich vooral intern en langs informele wegen, in plaats van langs formele organisatiekanalen. Een gevaar hiervan is dat kennis – onvolgroeid nota bene – blijft 'plakken' binnen een beperkte groep, in plaats van dat deze wordt gedeeld met 'het collectief' (met andere groepen, met organisatieonderdelen of met het landelijk niveau). Stickiness is een term die in dit verband wordt gebruikt.[15]

Travelling of ideas

Een ander punt is dat de geloofwaardigheid van een vertelling nauw verbonden is met de status en het gezag van de verteller. Zo is een verhaal uit de mond van persoon A meer waard dan hetzelfde verhaal uit de mond van persoon B. In die zin is er dus geen sprake van objectiveerbare verhalen. Ze zijn, met andere woorden, niet controleerbaar en in die zin ook niet meetbaar. Bovendien is er een zekere onvoorspelbaarheid in de verhaalontwikkeling en in de betekenis die mensen aan de verhalen geven. Achteraf kunnen verhalen dan ook hoogst ineffectief blijken te zijn, terwijl ze tegelijkertijd een oneigenlijke overtuigingskracht kunnen hebben. Snowden noemt dit het *story virus*, de vatbaarheid voor onverhoopt contraproductieve verhalen vanwege de sterke aantrekkingskracht ervan.[16] De effecten van storytelling zijn niet tot in detail te voorspellen. Verhalen brengen ons dan ook niet van een *ist*- naar een *soll*-situatie, maar van *ist* naar *etwas*. Verhalen gaan – net als vuur, of liever gezegd net als brand – hun eigen weg. Homan

FOTO ANP, R. NEDERSTIGT

De Brandweer Flevoland, hier bij een oefening, heeft een methodiek van storytelling ontwikkeld die veelbelovend kan zijn voor het Veiligheidsmanagementsysteem van Defensie

12 E. Stolper, *Gut Feelings in General Practice*. PhD thesis (Maastricht, Universitaire Pers Maastricht, 2010) 12.
13 D.M. Boje, *Storytelling Organizations* (Londen, SAGE, 2008) 75.
14 J.G. Vermaak, *Plezier Beleven aan Taaie Vraagstukken. Werkingsmechanismen van vernieuwing en weerbarstigheid* (Deventer, Kluwer, 2009) 496.
15 G. Szulanski, *Sticky Knowlegde. Barriers to Knowing in the Firm* (Londen, SAGE, 2003) 12.
16 D.J. Snowden, 'The Paradox of Story' in: *Journal of Scenario and Strategy Planning* 1 (1999) (5).

gebruikt hierbij de term *travelling of ideas*.[17] Wie even niet goed oplet, merkt dat verhalen een eigen leven gaan leiden.

Storytelling als actieve leerinterventie

Verhalen kunnen dus vanuit zichzelf ontstaan binnen een gemeenschap en volgen daarna – als brand – hun eigen weg. Tot op zekere hoogte is dat ook de bedoeling. Lessen zijn nu eenmaal niet altijd even gemakkelijk van bovenaf op te leggen. Bovendien vloeit kennis idealiter niet enkel *top-down*, maar vooral tussen de eigen oren en binnen de eigen operationele ploeg. Waar de genoemde kanttekeningen in de vorige paragraaf wel op wijzen, is dat het ongericht spelen met verhalen misschien wel moet worden beschouwd als het spelen met vuur.

Het is de kunst om de meest bruikbare informele leerverhalen 'op te vangen' en door te geven aan anderen

Doordat ze, ondanks de eigenschap van mogelijke stickiness, ook zo maar als een lopend vuurtje door de hele organisatie heen kunnen wandelen, kunnen ze ook veel onbedoelde effecten teweegbrengen, zowel in positieve als in negatieve zin. Het organische karakter van verhalen, de spontane ontkieming ervan, is echter onontkoombaar.[18] Leergemeenschappen zouden in eerste aanleg dan ook organisch moeten groeien. Wel is het de kunst om daaruit vervolgens de meest bruikbare informele leerverhalen 'op te vangen' en door te geven aan anderen. Zo kan niet enkel op operationeel niveau de kennis vloeien, maar ook op tactisch en op strategisch niveau; tussen ploegen, teams en eenheden, maar ook tussen kazernes en schepen en vliegbases. In het meest ideale geval gaan de leereffecten zelfs ver daarbuiten, bijvoorbeeld tot in missiegebieden.

Verhalen zijn namelijk ook te gebruiken als actief gekozen (leer-)interventie om bewustwording en gedragsverandering binnen de organisatie in gang te zetten. Enerzijds zijn dat de formele verhalen, vertaald naar officiële doctrines, tactieken en overige procedures. Defensie heeft daarnaast veel kenniscentra en produceert na missies vaak rapporten met *lessons identified*. Voor een daadwerkelijk en snel lerende organisatie is het echter van belang om ook het vertellen en de verspreiding van de meer informele verhalen te faciliteren, om zo het lerend vermogen van de organisatie verder te vergroten. Defensie zou bijvoorbeeld de ontwikkeling van 'spontane en informele' leergemeenschappen kunnen stimuleren, evenals het ontkiemen, volgroeien en verspreiden van lokale leerverhalen. Daardoor kan er meer ruimte ontstaan voor leren en voor verandering van gedrag. Veelal gaat het om verhalen met lessen die het waard zijn om te leren, lessen die de formele organisatie echter niet verplicht op kan leggen, maar waarbij de formele organisatie haar mensen wel degelijk kan helpen een eigen weg te vinden in de (h)erkenning, de bewustwording en de reflectie op die lessen. Zo kan de organisatie bepaalde ontkiemde verhalen oppakken en opnemen in les- en leerstof. Een andere mogelijkheid is om ze op ad-hoc basis gericht uit te (laten) dragen, bijvoorbeeld na een dodelijk ongeval.

Storytelling binnen de defensieorganisatie

De luchtmacht heeft – voor haar luchtvarenden en aanverwante beroepsgroepen althans – al sinds jaar en dag een structuur waarin het gericht delen van meer informele verhalen met elkaar gemeengoed is. De betrokkenen zullen zich evenwel niet bewust zijn dat ze aan het fenomeen storytelling doen. Zo zijn alle luchtvarenden verplicht jaarlijks minimaal één vliegveiligheidsdag (de *flight safety awareness*-dagen) bij te wonen, waarop dit soort verhalen met elkaar gedeeld wordt (zie kader).

17 T.H. Homan, *Organisatiedynamica. Theorie en praktijk van organisatieverandering* (Den Haag, Sdu Uitgevers BV, 2005) 132.

18 Vermaak, *Plezier Beleven aan Taaie Vraagstukken*, 498.

Voorbeeld van een luchtvarende

'Ik weet het nog goed. Weliswaar niet meer precies welk jaar, maar de beelden staan nu nog steeds, zo'n 15 jaar later, haarscherp op mijn netvlies. Ik zie de man nog zo voor me. Ik denk dat het zo ongeveer mijn eerste 'flight safety awareness' dag voor helikopters was dat ze die Amerikaan hadden uitgenodigd voor een praatje. In de opleiding waren we meermaals op de hoogte gesteld van het belang van het dragen van brandwerende kleding tijdens het vliegen. Bovendien werd dit streng gehandhaafd binnen het squadron, mede vanwege een eerder fataal afgelopen ongeval met twee leden van dat squadron. Ik bedoel, dat zet je toch wel even op scherp. En toch, de brand in het Hemeltje op oudejaarsnacht in Volendam had nog niet plaatsgevonden en het daadwerkelijke belang van brandwerende kleding, het gevoel dat het ook echt levensreddend kan zijn, dat kwam bij mij pas na het praatje van die Amerikaan met zijn verwrongen gezicht. Het gevoel is bij mij daarna nooit meer weg gegaan. De enige keer dat ik daarna geen brandwerende kleding heb gedragen is toen ik een noodgedwongen afweging moest maken tussen bevangen te worden door hittestuwing in Irak vanwege een buitentemperatuur van meer dan 50 graden Celsius en de kans dat we een ongeval met brand zouden krijgen. Alle andere keren is er bij mij niet eens een spoor van twijfel geweest of ik die, zeker in het begin, kriebelige kleding wel aan wilde trekken. Dat gezicht, die man, zijn verhaal, de intonatie, de emotie, het slikken, de gevolgen van het niet dragen van een slip waar hij over vertelde.... Je kon het verbrande vlees bijna ruiken in de zaal, zo heftig kwam het verhaal binnen. Niet alleen bij mij. We hebben het er nog weken over gehad en het heeft lang geduurd eer er mensen op het squadron verschenen die dit praatje niet hadden meegemaakt en die, ongelooflijk maar waar, zomaar in hun katoenen t-shirtje onder hun overall de helikopter in stapten....'

Daarnaast worden uit voorvallen getrokken lessen vaak direct teruggevoerd naar de in de loopbaan van een luchtvarende periodiek terugkerende supervisie- of *crew resource management* (CRM)-trainingen, waaraan alle bemanningen verplicht deelnemen. Sinds enkele jaren gelden vergelijkbare regels voor het luchtvaartsonderhouds-, het gevechtsleidings- en het luchtverkeersleidingspersoneel van het Commando Luchtstrijdkrachten (CLSK), evenals voor al het equivalente maritieme personeel dat het CLSK aanstuurt.
Deze structuur bij de luchtmacht is hoogstwaarschijnlijk deels terug te voeren op haar algemene connectie met de luchtvaartindustrie, waar veiligheid en het delen van veiligheidsinformatie van oudsher hoog op de agenda staat. Ook de andere krijgsmachtonderdelen kennen echter structuren waarin informatie op een vergelijkbare wijze wordt gedeeld, al is dat niet altijd specifiek veiligheidsinformatie.
Zo gebruikt het LOCKMar storytelling regelmatig als feedbackmechanisme om te interveniëren op processen en procedures. Hierbij nodigt het betreffende (management)team gericht functionarissen uit om hun indrukken en ervaringen in verhaalvorm te delen. Deze functionarissen worden bij het opstellen van hun verhaal begeleid door een specialist in deze methode. Na het verhaal volgt geen discussie, maar trekt het team uit het verhaal zijn eigen conclusies ter verbetering van hun organisatieprocessen.
Andere voorbeelden van het gebruik van storytelling zijn instructeurs en docenten die bepaalde lesstof vaak koppelen aan hun eigen ervaringen. Door de vele missies van de afgelopen decennia is dit alleen maar toegenomen, getuige ook de vele (ex-)defensiemedewerkers die via (auto)biografische boeken persoonlijke ervaringen delen. Zo publiceerde Jos Groen vorig jaar *Task Force Uruzgan*,[19] maar ook veel andere auteurs zoals Solkesz, Op de Haar en Roelen hebben hun ervaringen in missiegebieden op (auto)biografische wijze opgetekend.[20] Daarnaast zijn er de vele *YouTube*-filmpjes en andere berichtgevingen op de sociale media die ieder op hun eigen wijze kenmerken van storytelling in zich hebben.

19 J. Groen, *Task Force Uruzgan* (2006-2010). 'Getuigenissen van een missie' (Doorn, 2012).
20 A. Solkesz, *Hier Romeo. We Gaan Rijden!* (Rijswijk, Début, 1998); A.J. op de Haar, *De Koning van Tuzla* (Amsterdam, Querido, 1999); N. Roelen, *Soldaat in Uruzgan* (Amsterdam, Carrera, 2009).

Voorbeeld van een brandbestrijder

'Het is 25 december 2003 omstreeks half vijf in de ochtend … ik stond achter in de woning om een ventilatieopening te maken. Harry en Maikel waren voor in de woning bezig met het dichtdraaien van de hoofdgaskraan. Plotseling hoorde ik een doffe klap. Het leek op het aanslaan van een oude badgeiser. Met mijn gezicht naar het raam zag direct een blauwe vlam om mij heen. Uit reflex ben ik omgedraaid. En toen, toen hoorde ik helemaal niets meer, maar voelde een enorme druk op mijn lichaam ontstaan. Ik zag door de vlammen heen dat Harry door de druk tegen de muur was aangegooid. Maikel was boven op Harry gedoken. Hij drukte zijn gezicht in zijn lichaam om z'n eigen gelaat te beschermen. Ik voelde dat er op mijn hele lichaam en vooral op m'n gezicht een enorme hitte ontstond. Ik probeerde te kijken en zag een grote vuurzee om ons heen. Op dat moment stortte de wand naast de deur in. Ik zag dat Harry enkele stenen van zichzelf afgooide en probeerde op te staan. We hebben ons door de brandende massa en puin naar buiten weten te werken. Toen we buiten waren keek ik Harry recht in zijn gezicht aan. Het enige wat ik zag, waren losse vellen in zijn gezicht. Daarna stortte hij in en viel zeer ongelukkig in het trappenhuis van de flat. Samen met Maikel heb ik Harry op de trap onder de schouders gepakt en dacht ik bij mijzelf … SH*T … we zijn buiten … we hebben het overleefd.
Ondanks mijn gevoelens van schaamte is dit een deel van mijn verhaal van de Binnendijk dat ik graag met u deel. Twee brandweercollega's en ik raakten hier gewond bij een gasexplosie in een appartementencomplex. Bij velen is deze nacht, ook in emotionele zin, sterk blijven 'plakken'. Harry en ik werden met tweede- en derdegraads brandwonden opgenomen in het brandwondencentrum van Groningen. Maikel kon na behandeling in het ziekenhuis naar huis. Collega's buiten het wooncomplex dachten dat niet wij er levend uit zouden komen. De kracht van de explosie en de daaropvolgende uitslaande brand waren zo heftig dat zowel de voor- als de achtergevel volledig werden weggeslagen en de vlammen naar buiten sloegen. Wij zijn letterlijk vanuit het vuur naar buiten gestapt. Zo rijk als ik mijn verhaal hier beschrijf, zo zweeft het door de 'informele' organisatie.'
In meer formele zin is dit verhaal ondertussen opgepikt en gebruikt als één van de rolmodellen in het onderzoek Veiligheidsbewustzijn bij Brandweerpersoneel dat in 2004 is uitgevoerd in opdracht van de Inspectie Openbare Orde en Veiligheid (OOV). Daarnaast worden de hieruit getrokken lessen op het gebied van het gebruik van de explosiegevaar-meter, werkafstanden en de benaderingswijze van objecten, het maken van taak-/risico-analyses en de aandacht voor 'routine' in optreden tot op heden gebruikt in onze veiligheidsvorming en –trainingen.

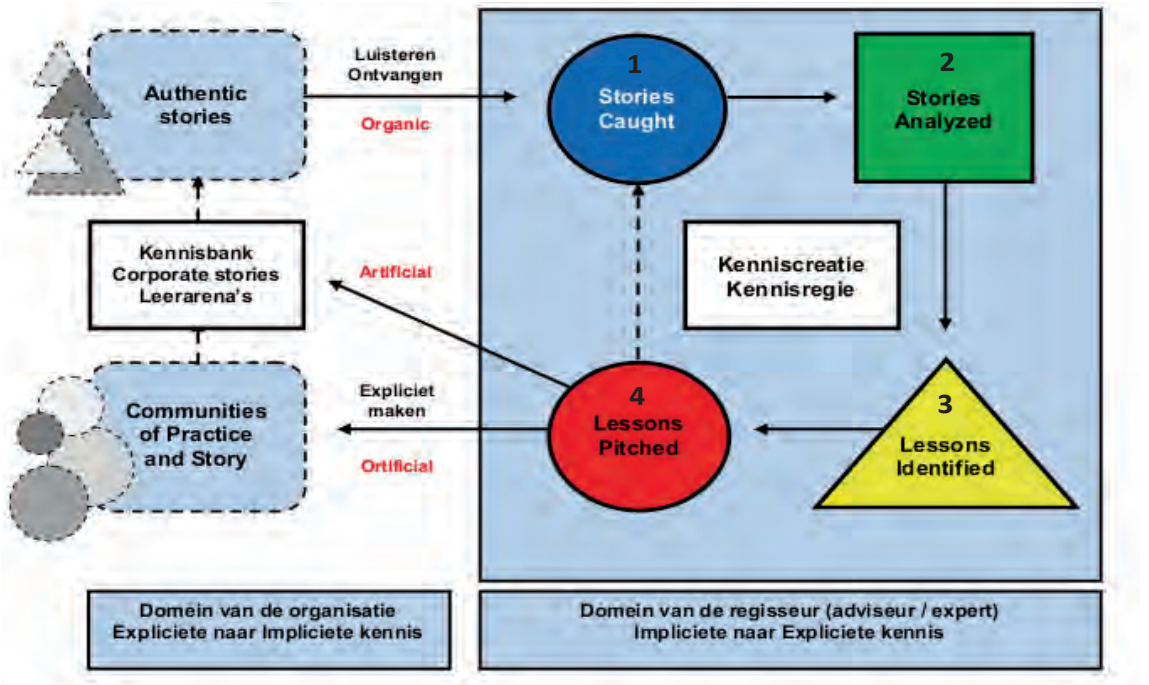
Bovengenoemde voorbeelden uit de defensieorganisatie passen niet allemaal één-op-één in de contouren van het fenomeen storytelling. Wat deze voorbeelden echter wel duidelijk maken is dat Defensie aan het gebruik van verhalen op zich een grote waarde toekent. Zo zal generaal Van Uhm niet voor niets voor de verhaalvorm hebben vernomen om op de TEDx van Amsterdam in 2011 zijn keuze voor het instrument om de wereld te verbeteren – een geweer – toe te lichten. Defensie past dus – ongemerkt wellicht – de technieken van storytelling toe, maar kan nog bewuster richting geven aan het fenomeen. Een verdere uitwerking van het principe en de eventuele toepassing ervan binnen Defensie ligt dan ook voor de hand.

Bewust gebruik van storytelling

Tijdens het onderzoek naar storytelling bij de Brandweer Flevoland gaven leidinggevenden aan dat zij in hun besluitvormingsproces in eerste instantie eigenlijk altijd terugvielen op het eigen referentiekader en dan vooral op hun persoonlijke ervaringen met vergelijkbare incidenten of op de eigen trainingsmomenten. Zij gaven echter ook aan dat zij verhalen van collega's die in de organisatie dichtbij hen stonden en die op diverse informele podia verteld waren, zeer bewust meenamen wanneer zij onder druk besluiten moesten nemen.[21]

Een voorbeeld hiervan zijn de verhalen naar aanleiding van een fatale brand in 2008 in de Drentse plaats De Punt. Op 9 mei dat jaar ontstond op een scheepswerf een zeer grote brand, waarbij drie brandweermannen om het leven kwamen. Veel verhalen naar aanleiding van deze dramatische brand zijn na afloop intensief gedeeld, zowel onderling als landelijk. Een merkbaar gevolg hiervan is dat bevelvoerders bij complexe branden in bedrijfspanden nu veelal defensiever op branden inzetten dan voorheen. De brand bij De Punt heeft een omslag teweeggebracht in het 'doctrine-denken' van de brandweer op het gebied van brandbestrijding in industriële gebouwen.
Een ander voorbeeld van storytelling naar aanleiding van een brand is weergegeven in het kader.

21 J.F. Van Opstal, *Storytelling. A lifesaving tool for firefighters*. Master thesis (Sioo, Interuniversitair Centrum voor Organisatie- en Veranderkunde (Advanced Change Methodologies) 2012).



Schema 1

Als de effecten van storytelling ook bij andere organisatieonderdelen moeten 'landen', dan zullen er op de een of andere manier sterkere verbanden moeten worden gecreëerd tussen de leden van die onderdelen. Dan zullen die medewerkers meerdere loyaliteiten moeten ontwikkelen, zodat ze zich niet enkel met elkaar verbonden voelen vanuit het lidmaatschap van hun eigen groep of werkeenheid, maar bijvoorbeeld ook vanuit meer specialistisch georiënteerde of ranggebonden verbanden. Op die manier kunnen er, spontaan door de organisatie heen, wat Lave en Wenger *communities of practice* noemen ontstaan.[22] Een spontane intervisiegroep van collega's die elkaar vinden vanuit een bepaalde werksituatie of passie is daar een concreet voorbeeld van. Onder voorzichtige regie kunnen deze verbanden echter ook actiever worden bewerkstelligd. Bij de luchtmacht en de marine zouden, behalve uiteraard leidinggevenden, de respectievelijke veiligheidsorganisaties hier een taak in kunnen hebben. Bij de landmacht ligt hier wellicht een rol voor commandanten en kenniscentra.

Een mogelijk stappenplan

Het hoofddoel van de studie van Van Opstal was het onwikkelen van een werkbaar concept om het informele leerverhaal uit de organisatie te vangen en te 'regisseren' en zo het lerend vermogen en het bewustzijn van de organisatie te vergroten. De verhalen zelf vormen daarbij het startpunt van een dialogisch proces.[23] De voorgestelde methodologie ligt in het *storycatching* en *lessons pitching*, oftewel in het vangen van de (informele) verhalen en de daaruit te trekken lessen, om die lessen vervolgens onder geleide weer terug te voeren naar (delen van) de organisatie.[24] Bij voorkeur gebeurt dit bij het gelijktijdig stimuleren en faciliteren van wat Van Opstal *communities of practice and story* (COPS) noemt. Hij heeft dit alles in een cyclisch proces van kenniscreatie en kennisregie gevat (zie schema 1).

22 J. Lave en E. Wenger, *Situated Learning. Legitimate Peripheral Participation* (Cambridge, Cambridge University Press, 1991).

23 T.A. Abma, 'Werken met narratieven. Verhalen en dialoog als methoden voor praktijkverbeteringen' in: Boonstra & Caluwé, *Interveniëren en Veranderen*, 82.

24 Van Opstal, *Storytelling*, 23.

Het hele proces dient uiteraard – hoewel met 'zachte hand' – geregisseerd te worden door een kennisregisseur.

Stap 1. Vangen en duiden
Het vangen van een geschikt verhaal is een delicate opdracht. Een kennisregisseur moet goed kunnen luisteren via formele, maar vooral ook via informele kanalen. Verhalen worden bijvoorbeeld opgevangen in gesprekken, tijdens observaties, in trainingen en tijdens oefeningen. De kennisregisseur zal daarom het vertrouwen moeten genieten en in staat moeten zijn de verhalen te duiden en op waarde te schatten; welk verhaal is wel en welk verhaal is niet geschikt om als startpunt te dienen van een dialoog die teruggevoerd kan worden naar de organisatie? Deze vaardigheid is lastig te definiëren maar berust op kwaliteiten zoals 'verhaalvaardigheid'. Zij berust eerder op kwaliteiten als 'verhaalvaardigheid', gezond verstand en – bovenal – intuïtie voor wat praktisch relevant is of zou kunnen zijn. Zaken als het aanwakkeren, het voeden en/of het ontwikkelen van het lerend vermogen van (leden van) de organisatie zijn hierbij doorslaggevend.

Bij het identificeren gaat het er om te leren lessen aan te wijzen die zullen worden omgezet in het uiteindelijk te pitchen verhaal

Stap 2. Filteren en analyseren
Na de vangst van het ruwe verhaal filtert de kennisregisseur eerst wat van de specifieke gebeurtenis wel en niet bruikbaar (te maken) is. Daarbij kijkt hij onder meer naar de mogelijkheden tot (het creëren van) een pakkende verhaallijn. Zo dient het verhaal authentiek te zijn en ook zo gebracht te kunnen worden. Functiegebonden en andere karakteristieken van direct en indirect betrokkenen spelen hierin een grote rol, evenals de transparantie in de dilemma's en worstelingen waar zij mee te maken hebben gehad en de afwegingen die zij daarbij al dan niet hebben gemaakt. Verder is het belangrijk te kijken naar de emoties die een verhaal oproept, om zo in te schatten in hoeverre het verhaal op betrekkingsniveau zijn uitwerking zal hebben. Daarna volgt een analyse naar de meer formele leermomenten. Deze analyse dienen meerdere deskundigen uit te voeren, zodat er ruimte ontstaat voor nieuwe betekenisgeving aan (elementen van) de voorbije gebeurtenis en voor kenniscreatie. Vervolgens vindt clustering naar onderwerp of thema van geleerde lessen plaats, zo mogelijk passend bij de (operationele) werkprocessen van de organisatie.

Stap 3. Identificeren
Bij het identificeren gaat het er om de te leren lessen of *best practices* aan te wijzen die zullen worden omgezet in het uiteindelijke te pitchen verhaal. Vervolgens wordt het verhaal, in 'co-creatie' met degene die het ruwe materiaal heeft aangeleverd en in dialoog tussen regisseur en verteller, narratief 'opnieuw' geconstrueerd en voor verspreiding (pitching) gereedgemaakt.

Stap 4. Valideren en aanbieden
Om de procedure van storytelling binnen een organisatie te laten welslagen is dit wellicht de allerbelangrijkste stap. Voordat de geïdentificeerde les(sen) in verhalende vorm wordt aangeboden (pitching) aan de verschillende (informele) communities of practice and story, dient een validatie op authenticiteit te worden uitgevoerd. Hierbij wordt gecontroleerd dat de leverancier van het ruwe materiaal, de uiteindelijke eigenaar van het verhaal, zich volledig herkent in wat zal worden gepitched. Na deze validatie gaat de 'co-creatie' de organisatie in en wordt het proces verder 'losgelaten', op weg naar het vangen en duiden van het volgende verhaal.

Storycatching & storypitching
Naast het doorlopen van bovengenoemd stappenplan zijn nog enkele andere zaken van belang, zo stelt Van Opstal. De kennisregisseur dient namelijk (het ontstaan van) de communities of practice and story te stimuleren en de (informele) leerruimte te faciliteren waar

verhalen en leerervaringen elkaar ontmoeten. De regisseur voedt de kennisdeling en kennisontwikkeling door deze ontmoeting te initiëren. Net als in het theater staat de regisseur niet zelf op het toneel, maar faciliteert hij de 'acteurs', degenen die het verhaal inbrengen. Lukt dat niet, dan zoekt de regisseur naar de juiste persoonlijkheden om het verhaal aan te bieden. Dat zijn 'pitchers', natuurlijke vertellers binnen de groep of gemeenschap die in staat zijn verhalen van anderen te brengen. Bovendien zijn zij in staat reflectie te creëren als een interactieve gebeurtenis tussen leden van zowel binnen als buiten het eigen organisatieonderdeel. Het meest krachtige blijft echter om de eigenaar zelf zijn of haar verhaal te laten vertellen. Want hoe dichter het verhaal bij de verteller blijft, hoe beter deze de luisteraars mee kan nemen in zijn of haar rol in het verhaal; hoe beter de verteller in staat is om de daar aan gekoppelde emoties over te brengen, de betekenis van het verhaal en de waarde (de geleerde les) die daar aan gegeven dient te worden.

Discussie en conclusie

Storytelling is uitdrukkelijk geen 'managementtool' dat een gegarandeerde empirische uitkomst kent. Een overzichtsartikel over het schoolse gebruik van narratieven verwoordt dit bijzonder krachtig: 'The actual uses of narrative and story in adult teaching and learning are literally unlimited because they arise from infinite expressions of interpretive interplay among teachers, learners, and content. And so we cannot reduce narrative into a handy toolkit of teaching techniques.'[25] Toch heeft het instrument zoals dat hier gepresenteerd is de potentie om het 'collectieve geheugen' van de organisatie te dienen. In 2009 heeft Defensie het Veiligheidsmanagementsysteem Defensie (VMSDef) ingericht. De reeds ingestelde VMS-procedures zijn voornamelijk gebaseerd op 'harde' – op beheersing en controle gebaseerde – managementtechnieken. De procedure voor het defensiebreed melden en registreren van voorvallen[26] is hier een voorbeeld van, maar heeft nog geen echte vlucht genomen. Dit zou kunnen worden geweten aan het gebrek aan mogelijkheden voor het opvolgen van de meldingen. Het meldingssysteem is echter bovenal een formeel instrument, dat niet actief op zoek gaat naar informatie. Het actualiseren van risicomodellen is echter van levensbelang, vooral in hoog-risico organisaties zoals Defensie. De methodiek van storytelling zoals die in dit artikel is voorgesteld lijkt dan ook veelbelovend om aan het arsenaal aan VMS-instrumentarium van Defensie toe te voegen.
Storytelling wordt binnen Defensie al toegepast, maar veelal onbewust. Wellicht dat dit artikel aan kan zetten tot een meer bewust gebruik ervan en tot de inzet bij het creëren van een zo veilig mogelijke werkomgeving, ook (of eigenlijk vooral) daar waar onder risicovolle omstandigheden dient te worden geopereerd. Storytelling stelt de organisatie beter in staat afwegingen te maken tijdens besluitvorming onder en over dit soort omstandigheden.

De voorgestelde methode is weliswaar een nog niet gevalideerde systematiek. Voor zover bekend bestaat die ook (nog) niet, in ieder geval niet specifiek voor organisaties die werken met hoog-risico processen zoals brandweer en Defensie. Het is daarom aan te raden te kijken of Defensie een rol zou kunnen en willen spelen in dit validatieproces, bijvoorbeeld als onderdeel van een meer proactief georiënteerd eigen veiligheidsbeleid. Een mogelijkheid is het uitvoeren van een *pilot* storytelling in nauwe samenwerking met de brandweerorganisatie, waarbij ervaringen van beide organisaties naast elkaar worden gelegd onder gelijktijdige uitwisseling van overige kennis en ervaringen. ■

25 M. Rossiter, 'Narrative and Stories in Adult Teaching and Learning' in: *Educational Resources Information Center* 'ERIC Digest (2002) (241) 2.

26 MP 12-100 *Veiligheidsmanagementssysteem Defensie* (VMSDef), Procedure 7: Melden en registreren van voorvallen.

Het begin van eeuwige oorlog

Op weg naar de eeuwige vrede?

Twee eeuwen geleden verschenen de geschriften van Von Clausewitz en Kant, die nog steeds veel invloed hebben op het westerse denken over oorlog en vrede. Kant was van mening dat een wereldvrede realiseerbaar was. Door het proces van integratie leek Europa in de periode 1945 – 2000 flinke stappen te zetten op weg naar een vreedzame Kantiaanse wereldgemeenschap. Er was sprake van een afname van de duur van conflicten, en een steeds geringer dodental per conflict. Volgens de auteur is de 'war on terror', die is uitgebroken na de aanslagen van 9/11, een heuse oorlog. Oorlog is dus zeker de wereld nog niet uit. Hoe komt het toch dat Kant ongelijk heeft gekregen?

*Prof. dr. B.G.J. de Graaff**

Het moderne westerse denken over oorlog en vrede is sterk bepaald door de geschriften van twee Pruisen die ongeveer twee eeuwen geleden verschenen: Carl von Clausewitz' in 1832 postuum verschenen Vom Kriege ('Over de oorlog') en Immanuel Kants *Zum ewigen Frieden - Ein philosophischer Entwurf* ('Naar de eeuwige vrede') uit 1795. In dit laatste geschrift betoonde Kant zich niet alleen voorstander van wereldvrede, hij meende dat deze ook realiseerbaar was.[1]

'Als van iemand gezegd kan worden dat hij de vrede heeft uitgevonden als meer dan een vroom streven, was het Kant', aldus de Britse militair historicus Michael Howard in zijn beschouwing *The Invention of Peace* ('De uitvinding van de vrede').[2]

Non-interventie beginsel

'De wijze van Königsberg', zoals Kant wel werd genoemd, somde enkele voorwaarden op voor zo'n mondiale vredestoestand. Net als de Engelse filosoof Thomas Hobbes een eeuw eerder, meende Kant dat oorlog de natuurlijke toestand was van mensen. Kant bleef echter niet steken in dit pessimisme. Hij meende dat een internationale aanvulling op het maatschappelijk verdrag van Rousseau politieke gemeenschappen kon weerhouden van het voeren van oorlog. Zo zou ten slotte een niet-ideale wereld veranderen in een ideale.

Onderdeel van zo'n aanvullend verdrag was het beginsel van non-interventie: staten zouden zich niet in elkaars aangelegenheden mogen mengen. Daarom was slechts zelfverdediging door weerbare burgers geoorloofd als vorm van oorlog; sluipmoord, gif mengen, uitlokking van verraad en soortgelijke oneervolle krijgslisten waren dat, aldus Kant, niet.

Verder zou tussen staten op basis van vrijwilligheid een internationale federatie tot stand

* De auteur is als hoogleraar verbonden aan de faculteit militair operationele wetenschappen van de Nederlandse Defensieacademie

1 Voor een Nederlandse vertaling met inleiding zie I. Kant, *Naar de eeuwige vrede. Een filosofisch ontwerp*, vert.: Th. Mertens en E. van Elden; voorwoord, inleiding en annotaties: Th. Mertens.

2 M. Howard, *The Invention of Peace. Reflections on War and International Order*, New Haven/London 2000, 31.

komen, een soort vredesbond, aangezien het lonkend perspectief van vermeerdering van welvaart zich tegen oorlog keerde en mensen en staten (Kant sprak van 'republieken') dus uit welbegrepen eigenbelang voor een internationaal gegarandeerde vrede zouden kiezen. Op grond van wat Kant betitelde als het 'kosmopolitisch recht' zouden staten gastvrijheid moeten verlenen aan burgers van andere staten, maar met behoud van hun oorspronkelijke nationaliteit. Kant bepleitte noch voorzag dus een wereldburgerschap.

Wie tussen 1945 en 2000 in West-Europa leefde, kon het idee hebben dat Kant gelijk kreeg. Door het proces van integratie leek Europa een flinke stap voorwaarts te zetten naar de vreedzame Kantiaanse wereldgemeenschap, zeker als deze ontwikkeling ook nog eens model zou staan voor regionale integratieprocessen elders in de wereld.

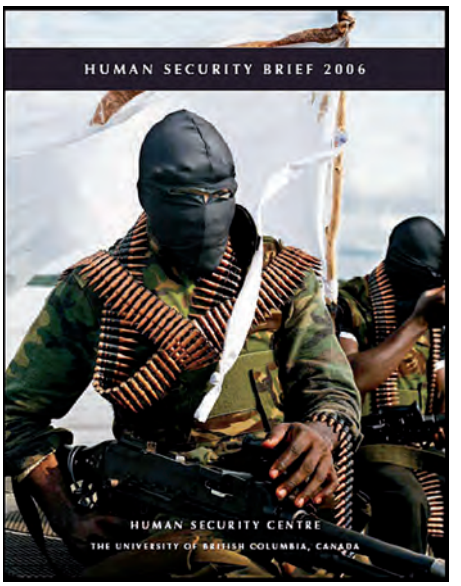
Afname van conflicten

De term 'debellicization' deed zijn intrede om een situatie te beschrijven waarin oorlog als instrument uit het politieke woordenboek leek te zijn verdwenen.[3] Vanaf 2005 verschenen vanuit Canada positief getinte rapporten van het *Human Security Report Project*, die wezen op onder meer de afname van de duur van conflicten en het steeds geringere dodental per conflict, al werden die rapporten in de loop van de tijd toch iets somberder: het aantal conflicten waarbij staten betrokken is blijft de laatste jaren gelijk, ongeveer dertig tot veertig, en het aantal niet-statelijke conflicten vertoont een licht stijgende tendens.[4]

Dit zou men echter kunnen zien als een conjuncturele dip in een wereldhistorische trend van afname van geweld, zoals die is geconstateerd door de Canadees-Amerikaanse evolutiepsycholoog Steven Pinker in zijn magnum opus *The Better Angels of Our Nature. Why Violence Has Declined*.[5]

In oorlog zonder het te weten[6]

Enkele jaren geleden, teruggekomen van een vakantie, zo'n moment waarop de wereld nog net



Rapport HSRP

wat mooier lijkt dan die is omdat ik mij dan verstoken houd van het wereldnieuws, werd ik bij thuiskomst overvallen door een Journaalbericht waarin een persofficier naar aanleiding van een terrorismeproces sprak over hulpverlening aan de vijand. Wat nu? Had ik tijdens mijn vakantie het uitbreken van een oorlog gemist?

Nee, het was anders. Ik had mij niet gerealiseerd dat de *war on terror* een echte oorlog was. Net als vele anderen had ik, toen president Bush direct na de aanslagen van 11 september 2001 verklaarde 'Ik wil dat iedereen begrijpt dat we in oorlog zijn en zullen blijven totdat dit over is',[7] geredeneerd dat dit 'natuurlijk' geen echte oorlog was.[8]

3 Vgl. W.J. Bennett, *Why We Fight. Moral Clarity and the War on Terrorism*, Washington D.C. 2003, 49; E.N. Luttwak, *Strategy: A New Era? The Tanner Lectures on Human Values Delivered at Yale University*, October 11 and 12, 1989, 48, http://tannerlectures.utah.edu/lectures/documents/Luttwak98.pdf. Zie ook Howard, Invention,100.

4 http://www.hsrgroup.org, laatstelijk Human Security Report Project, *Human Security Report 2012: Sexual Violence, Education, and War: Beyond the Mainstream Narrative*, Vancouver 2012.

5 S. Pinker, *The Better Angels of Our Nature. Why Violence Has Declined*, New York 2011. Zie ook http://www.sg.uu.nl/nieuwsblog/2013/05/07/ons-betere-ik.

6 S. Metz en Ph. Cuccia, Defining War for the 21st Century. 2010 Strategic Studies Institute Annual Strategy Conference Report, 2011, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1036.pdf, 8: 'How Do We Know That We Are at War?'

7 Geciteerd in R.A. Clarke, *Against All Enemies. Inside America's War on Terror*, New York 2004, 24.

8 Vergelijk. J. Mann, *Rise of the Vulcans. The History of Bush's War Cabinet*, New York etc. 2004, 304.

De *war on terror* is echter wel degelijk een oorlog gebleken, met echte militairen en met echte gesneuvelden, waarin het adagium werd: 'kill or be killed'.[9] Binnen een etmaal na de aanslagen van 9/11 had de NAVO voor het eerst in haar bestaan artikel 5 van het Handvest ingeroepen. Drie dagen na de verwoestende aanslagen machtigde het Amerikaanse Congres president Bush militair geweld te gebruiken tegen alle staten, organisaties en personen die op de een of andere manier bij de aanslagen betrokken waren geweest. Amerika was, in de woorden van de latere NAVO-ambassadeur Ivo Daalder, 'ontketend'.[10]

'Lange oorlogen'

Het heeft onder meer geleid tot de, op het Vietnam-conflict na, twee langste aaneengesloten oorlogen waarin de Amerikanen ooit verzeild zijn geraakt: de oorlogen in Afghanistan en Irak. Weliswaar had Irak niets te maken met de aanslagen van 11 september 2001, maar de Amerikaanse regering legde dit verband wel.[11]

Maar de oorlog tegen het terrorisme strekt zich nog veel verder over de wereld uit. Zij woedt bijvoorbeeld ook in Pakistan, Jemen, Somalië en Nigeria.[12] Het is een echte 'global war against terrorism'.[13] Het duo terrorisme en oorlog vormde samen met armoede en problemen betreffende energie, water, voedsel en milieu, dan ook een van de zes thema's die uiteenlopende referentiegroepen verspreid over de wereld in de jaren 2002 en 2003 telkens opnieuw aanwezen als de zes grootste problemen

FOTO US DEPARTMENT OF DEFENSE

Operatie 'Enduring Freedom'. 'De Verenigde Staten zijn bezig met wat een lange oorlog zal worden', aldus de Strategic Defense Review

voor de komende vijftig jaar.[14] Oorlog was dus zeker de wereld nog niet uit. De Britse publicist Jason Burke schatte het aantal dodelijke slachtoffers dat tussen 2001 en 2012 was gevallen in de, zoals hij ze noemt, '9/11 wars' op een kwart miljoen; het aantal gewonden op een half miljoen.[15] De Amerikaanse *Strategic Defense Review van 2006* verklaarde in sobere bewoordingen: 'De Verenigde Staten zijn bezig met wat een lange oorlog zal worden'.[16] De *long war*[17] was de term die na enige tijd het begrip *war on terror(ism)* verving. Anderen spraken van een *global counterinsurgency* of hanteerden een scala aan begrippen die poogden het alomvattende karakter van het conflict te verbloemen danwel juist die verheimelijking bloot te leggen.

9 M.A. Ledeen, *The War Against the Terror Masters. Why It Happened. Where We Are Now. How We'll Win*, New York 2003, xvii.

10 I.H. Daalder & J.M. Lindsay, *America Unbound. The Bush Revolution in Foreign Policy*, Washington D.C. 2003.

11 Zie bijvoorbeeld de serie van Bob Woodward, *Bush at War, Plan of Attack, State of Denial,* New York 2003-2007.

12 Zie bijvoorbeeld C. Lynch, 'Is the U.S. Ramping Up a Secret War in Somalia?', *Foreign Policy*, 22 juli 2013; D. Axe, 'Reports: U.S. Military to Help Fight Nigerian Terrorists', *Wired*, 11 november 2011; 'U.S. drones dpy on Boko Haram', *Punch*, 25 mei 2013; B. Oladeji, 'Nigeria: United States Intensifies War Against Boko Haram, Others', *Leadership*, 20 juni 2013.

13 Bennett, Why, 27.

14 http://cnst.rice.edu/content.aspx?id=246.

15 J. Burke, *The 9/11 Wars*, London 2011, 505.

16 Geciteerd in Burke, *Wars*, 259.

17 Zie noot 15, 260.

De wereld als slagveld

Zij namen termen in de mond als *discrete military operations*[18], *protracted conflict*,[19] *low-level conflict*,[20] *military operations other than war*, *conflicts of wars far from declared war zones*, *internationalized non-international armed conflicts*,[21] *secret, hidden of clandestine wars* [22]. Of *conflicts*,[23] *stealth wars, remote-control wars*, oorlogen met een *light footprint*, *small wars*, *unconventional warfare, ever-expanding dirty wars* of *open-ended wars*.[24] Hoe dan ook, de wereld was '*a battlefield*', *een slagveld* voor dit type oorlogen geworden.[25] Degenen die hadden gezegd dat de strijd tegen het (islamistisch) terrorisme, na de Eerste en de Tweede Wereldoorlog en de Koude Oorlog, de Vierde Wereldoorlog zou voortbrengen, leken gelijk te krijgen.[26] Vanaf 1989 kwamen westerse legers vaker in actie dan tijdens enig decennium uit de Koude Oorlog, hetzij bij vredesoperaties, hetzij in de 9/11 wars.[27]

Eeuwige oorlog

Wat misschien wel het meest verbazingwekkend was, was dat er na 9/11 geen terugkeer was naar een 'normale toestand' of anders gezegd: oorlogsgesteldheid werd de normale toestand. Zoals een ouwe rot uit het Amerikaanse inlichtingenbedrijf een half jaar na 9/11 verklaarde: 'Ik ben nog iedere dag verrast, omdat ik dertig jaar lang heb geleerd dat na een crisis de toestand binnen zes tot acht weken weer normaal wordt. Maar deze lui [hij doelde op de regering-Bush] tonen geen tekenen van een verandering. […] Zij weigeren terug te keren naar een situatie van business-as-usual.'[28] Integendeel, Bush en zijn regering creëerden een mondiale tegenstelling die geen nuancering toeliet. Nadat Bush kort na de aanslagen van 9/11 in het Amerikaanse Congres had verklaard: 'Je bent óf voor ons óf voor de terroristen', zei hij het een jaar later nog eens: 'Er is geen neutraal terrein - geen neutraal terrein in de strijd tussen beschaving en terrorisme […].'[29]

Cyberwar

Hoewel ook nu nog de *war on terror* boven aan de veiligheidsagenda staat, dringen zich nieuwe prioriteiten in het westerse veiligheidsdenken op die eveneens de oorlog als normale toestand omhelzen: de oorlog tegen de georganiseerde misdaad, in de Amerikaanse strategie getypeerd als 'self-perpetuating associations of individuals' (zichzelf instandhoudende groepen individuen),[30] en *cyberwar*, al dan niet in combinatie.

Terwijl tal van strategen zich nog afvragen hoe groot de dreiging van *cyberattacks* is, woedt de *cyberwar* reeds in alle hevigheid, bijvoorbeeld tussen de Verenigde Staten en China, tussen de Verenigde Staten en Israël enerzijds en Iran anderzijds, tussen de Amerikaanse overheid en de georganiseerde misdaad en tussen *Anonymous* en staten als Israël of Turkije. [31]

18 M. Zenko, *Between Threats and War. U.S. Discrete Military Operations in the Post-Cold War World*, Stanford, CA, 2010.

19 J.J. Carafano & P. Rosenzweig, *Winning the Long War. Lessons from the Cold War for Defeating Terrorism and Preserving Freedom*, Lanham, MD, 2005, 15.

20 D.E. Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*, 244.

21 Chr. Jenks, 'Law from above: unmanned aerial systems, use of force, and the law of armed conflict', in: North Dakota Law Review, vol. 85 (2009), 649-671.

22 M. Mazzetti, *The Way of the Knife. The CIA, a Secret Army, and a War at the Ends of the Earth*, New York 2013, 4, 11, 13 en 100-101.

23 Sanger, *Confront*, 245.

24 J. Scahill, *Dirty Wars. The World is a Battlefield*, New York 2013, xxiv, 19 en 282-283.

25 Scahill, *Wars*.

26 Zie bijvoorbeeld A. de Marenches & D.A. Andelman, *The fourth world war; diplomacy and espionage in the age of terrorism*, New York 1992. Vgl. N. Podhoretz, *World War IV. The Long Struggle Against Islamofascism*, New York 2007; B. Tertrais, *War Without End. The View from Abroad*, New York/London 2005, 24; J. Woolsey, 'World War IV. Speech', 16 november 2002, http://www.globalsecurity.org/military/library/report/2002/021116-ww4.htm;Th. Wolton, *Quatrième Guerre Mondiale*, Paris 2005.

27 Vgl.Th.M. Barnett, *The Pentagon's New Map. War and Peace in the Twenty-First Century*, New York 2004, 3.

28 Mann, *Rise*, 313-314.

29 Geciteerd in Tertrais, *War*, 43.

30 *Strategy to Combat Transnational Organized Crime. Addressing Converging Threats to National Security*, Washington D.C. 2011, 0.

31 Zie S. Gorman & D. Yadron, 'Iran Hacks Energy Firms, U.S. Says', *The Wall Street Journal*, 23 mei 2013; C. Cohn, 'Will the U.S.-Iran Cyber Conflict Escalate?', *National Iranian American Council*, 7 augustus 2013; P. Paganini, 'The cyber capabilitie sof Iran can hit US', *SecurityAffairs*, 14 augustus 2013; Greenwald, G. en E. MacAskill, 'Obama orders US to draw up overseas target list for cyber-attacks', *The Guardian*, 7 juni 2013; M.J. Gross, 'Silent War', *Vanity Fair*, juli 2013; J. Zarate, *Treasury's War. The Unleashing of a New Era of Financial Warfare* (verschijnt binnenkort); E. Nakashima, 'Chinese hackers who breached Google gained access to sensitive data, U.S. officials say', *The Washington Post*, 20 mei 2013; 'Middle East in spotlight amid escalating cyber attacks', Alarabya.net, 19 mei 2013; T. Shanker en D.E. Sanger, 'U.S, Helps Allies Trying to Battle Iranian Hackers', *The New York Times*, 8 juni 2013; A. Egozi, 'Secret wars and why they avoid big conflagrations', *Israel's Homeland Securuty Home*, 12 August 2013; B. Dorgan, 'Cyber Terror Is the New Language of War', *Huffington Post*, 17 juli 2013.

Desillusie

Wie dacht dat al dit soort oorlogen zou stoppen met de machtswisseling Bush-Obama kwam bedrogen uit. Voor Obama gold niet minder dan voor Bush dat in het huidige tijdsgewricht 'de wereld […] een slagveld' is, 'en wij bevinden ons in oorlog'.[32] Vandaag de dag leven we, aldus de president in 2010, in 'een tijdperk zonder overgaveceremonieën.'[33] Obama maakte meer gebruik van *Special Forces* en *drones* dan zijn voorganger. In de eerste anderhalf jaar van zijn regering vergrootte hij het aantal landen waar Amerikaanse *special operation forces* actief waren van 60 naar 75.[34]

Drones werden Obama's 'geprefereerde drug'; hij was verliefd geworden op dit wapen, aldus insiders, en kreeg de bijnaam 'de drones-president'.[35] Terwijl tijdens de regering van

FOTO US DEPARTMENT OF DEFENSE

Obama maakt meer gebruik van Special Forces en drones dan zijn voorganger. Ook voor Obama geldt dat 'de wereld een slagveld' is

George Bush jr. enkele tientallen *drone*-aanvallen plaatshadden, vonden onder Obama's presidentschap tot nu toe honderden *drone*-aanvallen plaats, met duizenden doden, wwwaarvan een groot aantal in Pakistan, een land waarmee de VS officieel niet in oorlog waren.[36]

Wie meent dat de toespraak van Obama uit mei van dit jaar dit type oorlog zal beëindigen, staat net zo'n desillusie te wachten als degene die op dit gebied een verandering verwachtte van zijn aantreden. Voorlopig kondigt de regering-Obama aan dat de oorlog tegen Al-Qaeda nog 'ten minste tien tot twintig jaar' gaat duren; en dan de rest nog.[37] Voor wat specifiek de beëindiging van de drone-aanvallen in Pakistan betreft liet de regering-Obama intussen weten dat 'er geen exacte tijdslijn aan te geven valt' en intussen liep het aantal drone-aanvallen sinds de speech van Obama

32 Scahill, *Wars*, xxiii, 4, 183, 351; P. Baker, 'Obama's Turn in Bush's Bind', *The New York Times*, 9 februari 2013; S.L. Carter, *The Violence of Peace. America's Wars in the Age of Obama*, Philadelphia, PA, 2011, 64; G. Miller, 'As Obama defends counterterrorism tactics, he finds himself in Bush territory', *The Washington Post*, 9 juni 2013; B. Ramsey, 'On drones, Obama is Bush', *The Seattle Times*, 12 februari 2013.

33 Geciteerd in Metz en Cuccia, War, 14.

34 Scahill, *Wars*, 350 en 352-355; K. DeYoung & G. Jaffe, 'U.S. "Secret War" Expands Globally as Special Operation Forces Take Larger Role', *The Washington Post*, 4 juni 2010.

35 Vgl. Carter, *Violence*, xi en 169. J.A. Rodriguez, *Hard Measures. How Aggressive CIA Actions after 9/11 saved American Lives*, New York 2012, 251 en 255. Zie ook Sanger, *Confront*, 243-244, 252 en 254; Scahill, *Wars*, 244-247, 250-251, 263; A. Elshout, 'De Amerikaanse drone', *de Volkskrant*, 22 juni 2013.

36 International Crisis Group, Drones: *Myths and Reality in Pakistan*, Asia Report no. 247, 21 mei 2013; H.A. Crumpton, *The Art of Intelligence. Lessons from a Life in the CIA's Clandestine Service*, New York 2012,7; Rhe Bureau of Investigative Journalism, 'Covert War on Terror - the Datasets', http://www.thebureauinvestigates.com; Sanger, *Confront*, 244; Carter, *Violence*, 3; M. Bowden, *The Finish. The Killing of Osama bin Laden*, New York 2012, 67 en 71; J. Tandler, 'Known and Unknowns: President Obama's Lethal Drone Doctrine', Fondation pour la Recherche Stratégique, *Note no. 7/13*; N. Turse en T. Engelhardt, *Terminator Planet. The First History of Drone Warfare 2001-205*0, Marston Gate 2012; A. Wright, '"I protest": challenging the war policies of the United States', *Open Democracy*, 22 mei 2013.

37 'Text of President Obama's May 23 speech on national security (full transcript)', *The Washington Post*, 23 mei 2013; G. Dyer, 'Pentagon sees "war on terror" lasting 20 years', *Financial Times*, 17 mei 2013; A. Rosenthal, 'The Forever War', *The New York Times*, 17 mei 2013; Ch. Savage & P. Baker, 'Obama, in a Shift, to Limit Targets of Drone Strikes', *The New York Times*, 22 mei 2013; A. Ahmed, 'The Drone War is Far From Over', *The New York Times*, 30 mei 2013; G. Miller, 'Obama's new drone policy leaves room for CIA', T*he Washington Post*, 25 mei 2013; S.G. Stolberg, 'Wind Down the War on Terrorism? Republicans Say No', *The New York Times*, 26 mei 2013; Elshout, 'Drone'; Ph.Chr. Ulrich, Why Obama needs drones. *US Drone Policy during the Obama Administration*, Copenhagen 2013. Vgl. P. Miller, 'The War on Terror Must End - but Not Yet', *Foreign Policy*, 31 mei 2013.

op.[38] We zijn begonnen aan de eeuwige oorlog, er is *No End to War*.[39] *The Forever War*,[40] de *War Without End*,[41] de *Perpetual War* – om slechts naar een paar recente boeken te verwijzen – is hier en verdwijnt per definitie niet.[42]
De vraag is derhalve: waarom heeft Kant geen gelijk gekregen? Waarom zijn we de weg van de eeuwige oorlog ingeslagen in plaats van die van de eeuwige vrede? De redenen daarvoor zijn te vinden zowel in het feit dat aan Kants voorwaarden voor vrede niet is voldaan, als in het tijdgebonden karakter van zijn opvattingen.

Wat is oorlog?

Hoewel Kant in zijn vredesaanzet nergens een definitie van oorlog geeft, is duidelijk dat voor hem oorlogen beperkt waren tot eendimensionale, interstatelijke, gewelddadige conflicten die begrensd waren in tijd en ruimte. Hij hanteerde 'oorlog' in de traditionele betekenis die *Van Dale's* woordenboek er nog steeds aan geeft: 'strijd tussen twee of meer volken'. Intussen bestaan er ruimere definities die slechts het georganiseerde, doelbewuste en politieke karakter van de strijd en de (extreme) gewelddadigheid ervan benadrukken.[43] Zij bevinden zich binnen de nog ruimere kaders van de definitie die Von Clausewitz aan het fenomeen gaf toen hij schreef: 'Oorlog is een gewelddadige handeling om de tegenstander te dwingen onze wil in vervulling te doen gaan'.[44] Kant had nog geen zicht op het hedendaagse type multidimensionale conflicten met niet-statelijke actoren, zonder een formeel begin en eind van de gevechtshandelingen, gewapende conflicten die vaak de vorm aannemen van burgeroorlogen, *insurgencies* of zogeheten vredesoperaties, compleet met afdwinging, overigens juist typen oorlogen die bekendstaan om hun relatief lange duur.[45]

Nieuw type terrorisme

De strijd tegen het terrorisme, verklaarde de Amerikaanse minister van Defensie Donald Rumsfeld twee weken na de aanslagen van 9/11, zou niet eindigen met een beslissende slag of formele overgave. Het ging bij de strijd tegen het nieuwe type terrorisme namelijk om 'een brede, duurzame en veelzijdige inspanning die bijzonder en opvallend verschilt van eerdere inspanningen. Het ligt in de aard van het verschijnsel dat er niet op kan worden gereageerd met een massale aanval of invasie. Het is een veel subtieler, genuanceerder, moeilijker en schimmiger complex van problemen'.[46]
Niet alleen was de oorlog tegen het terrorisme een tamelijk 'vormloze'[47] strijd tegen een strijdwijze, vanaf het begin waren de doelen daarbij bovendien zo ambitieus dat een begrenzing in de tijd moeilijk was.[48] De vijand was divers en verspreid. Zoals Nederland eind negentiende eeuw militair optrad tegen onhandelbare zelfbestuursgebieden in Nederlands-Indië, zo stelden de recente Amerikaanse regeringen zich teweer tegen de mogelijkheden die *failed states* aan terroristen bieden: 'we moeten hen de vrijplaatsen ontzeggen overal waar we dat kunnen'; een opstelling die noodzakelijkerwijs een aantasting van soevereiniteit betekent.[49]

38 M.R. Gordon, 'Kerry, in Pakistan, Expresses Optimism on Ending Drones Strikes Soon', *The New York Times*, 1 augustus 2013; M. Mazzetti & M. Landler, 'Despite Administration Promises, Few Signs of Change in Drone Wars', *The New York Times*, 2 augustus 2013.
39 W. Laqueur, *No End to War. Terrorism in the Twenty-First Century*, New York 2003.
40 D. Filkins, *The Forever War. Dispatches from the War on Terror*, London 2008.
41 Tertrais, *War*.
42 B.W. Robbins, Perpetual *War. Cosmopolitanism from the Viewpoint of Violence*, Durham, NC, 2012; Scahill, *Wars*, 513.
43 Zie https://en.wikipedia.org/wiki/War of http://de.wikipedia.org/wiki/Krieg.
44 'Der Krieg ist […] ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen', C. von Clausewitz, *Vom Kriege*, Buch I, Kapitel 1, Abschnitt 2.
45 De negentig *insurgencies* die sinds de Tweede Wereldoorlog begonnen zijn duurden, als het al mogelijk was een eind vast te stellen, gemiddeld dertien jaar, W.L. Perry & J. Gordon IV, *Analytic Support to Intelligence in Counterinsurgencies*, Santa Monica, CA, 2008, 2-3.
46 Geciteerd in A. Simons & D. Tucker, 'United States Special Operations Forces and the War on Terrorism', Th.R. Mockaitis & P.B. Rich (red.), Grand Strategy in the War against Terrorism, London/Portland, OR, 2003, 77. Vgl. ook de woorden van nationale veiligheidsadviseur Condoleezza Rice op Fox News in november 2002: 'We're in a new kind of war, and we've made very clear that it is important that this kind of war be fought on different battlefields', geciteerd in Scahill, Wars, 78.
47 Vgl. N. Mailer, Why Are We At War?, New York 2003, 81-82.
48 Vgl. P. Gilbert, New Terror, New Wars, Edinburgh 2003, 44.
49 Paul Wolfowitz tegenover CNN, geciteerd in Scahill, Wars, 77. Vgl. B. de Graaff, 'Tegenbeeld en evenbeeld. Westerse interventies in falende staten toen en nu', M. Bloembergen en R. Raben (red.), Het koloniale beschavingsoffensief. Wegen naar het nieuwe Indië, 1890-1950, Leiden 2009, 295-319; Barnett, Map, 7; Bowden, Finish, 79-81; K. Cragin, 'The Strategic Dilemma of Terrorist Havens Calls for Their Isolation, Not Elimination', B.M. Jenkins and J.P. Godges (red.), The Long Shadow of 9/11. America;'s Response to Terrorism, Santa Monica, CA, 2011, 113-120; G. Spörl, 'Interview with Ahmed Rashid. The West Should "Change Its Approach to Failing States"', SpiegelOnline, 31 december 2012; Tertrais, War, 101.

Internet

En wat geldt voor *failed states* in de realiteit, is niet minder waar voor de virtuele werkelijkheid van het internet, ''s werelds grootste onbeheerste ruimte'.[50] Deze opstelling is een reactie op de democratisering van geweld, en van oorlogvoering in het bijzonder, een tendens waarbij zogeheten *super* of *hyper-empowered* individuen steeds beter in staat zijn een oorlog te beginnen en winnen.[51]

President Bush verklaarde dat de 'war on terror' weliswaar begon met 'Al-Qaeada maar daarmee niet eindigt. Die zal niet eindigen voordat elke terroristische groep die wereldwijd kan opereren gevonden, gestopt en verslagen is.' De president was zich er ten volle van bewust dat dit 'een langdurige veldtocht' vergde, 'een moeilijke strijd van onbepaalde tijdsduur'. Vice-president Cheney meende zelfs: '[Er] zal misschien wel nooit een eind aan komen. In elk geval niet tijdens ons leven.'[52]

FOTO US DEPARTMENT OF DEFENSE

Twee weken na 9/11 verklaarde Donald Rumsfeld dat de strijd tegen het terrorisme niet zou eindigen met een beslissende slag of formele overgave

Geen definitieve overwinning

Door de verscheidenheid aan groepen, die soms menen een wereldwijde, kosmische strijd te voeren, is het inderdaad moeilijk, zo niet onmogelijk een definitieve overwinning te behalen.[53] Wegens het ontbreken van concretere maatstaven voor overwinning en een onhelder begrip van de tegenstander kan zo'n oorlog inderdaad niet anders dan eindeloos zijn en moest het Amerikaanse strategische denken wel vervallen in het winnen van veldslagen in plaats van het behalen van strategische overwinningen.[54]

De introductie van de preventieve oorlog

Het gebrek aan begrenzing van de strijd in de tijd komt mede door het karakter van terrorisme. Een aanslag staat daarbij niet op zichzelf, maar houdt ook een dreiging of belofte in:

50 E. Schmidt en J. Cohen, The New Digital Age. Reshaping the Future of People, Nations and Business, New York 2013, 3. Zie ook G.C.M. Moura, Internet Bas Neighborhoods, Amsterdam 2013.

51 Th.L. Friedman, The Lexus and the Olive Tree, New York 2000, 14-15, 140, 192, 211, 269, 398 en 462; S. Gayken, Cyberwar. Das Internet als Kriegsschauplatz, München 2011, 195; F. Zakaria, The Future of Freedom. Liberal Democracy at Home and Abroad, New York 2003, 15-16; J. Robb, Brave New War. The Next Stage of Terrorism and the End of Globalization, Hoboken, NJ, 2007, 8, 19, 74 en 139-142; Laqueur, End, 10.

52 Geciteerd in G. Kolko, Another century of war?, New York 2002, 2-3. Zie ook Scahill, Wars, 48.

53 Zie Wolton, Guerre, 210; Tertrais, War, 95; R. Aslan, How to Win a Cosmic War. God, Globalization, and the End of the War on Terror, New York 2009, xix.

54 Zie M.M. Aid, Intel Wars. The Secret History of the Fight Against Terror, New York 2012, 153; R. Baer, 'Taliban Imposter: The US Doesn't Know Its Enemy', Time, 28 november 2010, http://www.time.com/time/nation/article/0,8599,2033376,00.html; Burke, Wars, xix en 501; B. Connable, Embracing the Fog of War. Assessment and Metrics in Counterinsurgency, Santa Monica, CA, 2012; Th.X. Hammes, The Sling and The Stone. On War in the 21st Century, St. Paul, MN, 2006, 225-226 en 230; R. Maddow, Drift. The Unmooring of Military Power, New York 2012, 210; J. Marcus, 'Spent force: Are wars still winnable?', iBBC News, 6 maart 2013; H.R. McMaster, 'The Pipe Dream of Easy War', The New York Times, 20 juli 2012; Metz en Cuccia, War, 12; Chr. Paul, 'Winning Every Battle but Losing the War Against Terrorists and Insurgents', B.M. Jenkins en J.P. Godges (red.), The Long Shadow of 9/11. America;'s Response to Terrorism, Santa Monica, CA, 105-111; Sanger, Confront, 28, 244, 422 en 435-436; Tertrais, War, 92; K. Patton, Sociocultural Intelligence. A New Discipline in Intelligence Studies, New York 2010; A. Strick van Linschoten en F. Kuehn, An Enemy We Created. The Myth of the Taliban/Al Qaeda Merger in Afghanistan, 1970-2010, London 2012; Turse een Engelhardt, Planet, 16-17, 25, 28; R.F. Worth, 'Can We Imagine the Life of a Terrorist?', The New York Times, 14 juni 2013; Zenko, Threats, 2.

na deze aanslag kan er nog één volgen. En sinds de jaren negentig van de vorige eeuw is die dreiging uitgebreid tot de mogelijkheid van een zogeheten CBRN-aanslag, een aanslag met een chemisch, bacteriologisch, radiologisch of nucleair karakter, waarop vergelding niet kan uitblijven. Sterker nog, vice-president Dick Cheney formuleerde de doctrine dat als er één procent kans is op een (nucleaire) dreiging van een terroristische groepering, de Amerikaanse regering daarop moet reageren 'als een zekerheid in termen van onze respons'.[55]

In soortgelijke termen verklaart een document van het Amerikaanse ministerie van Justitie getiteld 'Lawfulness of a Lethal Operation Directed Against a U.S. Citizen' ('Wettigheid van een dodelijke operatie gericht tegen een Amerikaans burger') dat een *drone*-aanval op een Amerikaans burger, waar dan ook ter wereld, gerechtvaardigd is, ook als er geen sprake is van 'onomstotelijk bewijs dat een specifieke aanval op Amerikanen zal plaatshebben in de nabije toekomst'.[56]

Anders dan ten tijde van de Koude Oorlog tegenover andere grote mogendheden zou *deterrence* (afschrikking) tegenover terroristen die niet bang zijn te sterven namelijk niet meer werken.[57] Waar ten tijde van de Koude Oorlog de angst voor een atomair conflict nog een rem was op oorlogvoering, is zij er nu een stimulans voor. Deze gedachtegang leidde tot de doctrine van *pre-emption*, zoals vastgelegd in de *U.S. National Security Strategy* van 2002.[58]
In de woorden van Bush: 'We moeten de strijd verplaatsen naar de vijand, zijn plannen ontwrichten en de ergste dreigingen te lijf gaan voordat zij de kans krijgen op te komen'.[59]

Diezelfde gedachte beheerst de Amerikaanse, en niet alleen de Amerikaanse, cyber-strategie.[60]
In de cyber-wereld, zo is het idee, werkt *deterrence* namelijk al even weinig.[61] Anders dan bij reguliere oorlogvoering overschrijdt men bij cyberwar bijna ongemerkt nationale grenzen. Cyberwars kennen geen slagvelden, maar *battlespaces*, waar de ene aanval de andere uitlokt en wereldburgerschap onbedoeld een realiteit is geworden.[62] Omdat zeker in de niet-virtuele wereld staten ertoe blijven doen, kunnen aanvallen in de virtuele wereld leiden tot militaire reacties in de reële wereld; dat recht behoudt de Amerikaanse regering zich althans voor.[63]

Hoe minder slachtoffers, des te meer en des te langere oorlog[64]

Persoonlijk zou ik een definitie van oorlog willen hanteren die de volgende elementen omvat: het onderscheid tussen twee of meer entiteiten die elkaar vijandig bejegenen op politiek, economisch of religieus gebied en waarbij in elk geval een van de partijen probeert de ander haar wil op te leggen, het georganiseerde karakter van de strijd en een zekere mate van bestendigheid van het conflict. In zo'n definitie zegt oorlog niets over de aantallen fysieke slachtoffers, over de duur van individuele conflicten of over de vraag of die oorlogen al dan niet 'officieel verklaard' zijn.

Oorlogen zonder doden

Oorlogen zonder doden zijn voorstelbaar, bijvoorbeeld als partijen uitsluitend gebruik-

55 R. Susskind, The One Perrcent Doctrine. Deep Inside America's Pursuit of Its Enemies Since 9/11, London 2006, 62 en 150; Carter, Violence, 31 en 33.
56 Scahill, Wars, 514 en 352.
57 Tertrais, War, 93.
58 Geciteerd in Mann, Rise, 329.
59 Carter, Violence,19; Daalder & Lindsay, America, 13, 119 en 121; Mann, Rise, 199-200, 202-203, 214 en 327.
60 Sanger, Confront, 247, 264-265 en 268; N. Shachtman, 'The Pentagon Project Makes Cyberwar as Easy as Angry Birds', Danger Room, 28 mei 2013; Th. Shanker, 'Pentagon Is Updating Conflict Rules in Cyberspace', The New York Times, 27 juni 2013; B. Schneider, 'Has U.S. started an Internet war?', CNN, 18 juni 2013; W. Strobel en D. Charles, 'With troops and techies, U.S. prepares for cyber warfare', Reuters, 7 juni 2013.
61 Sanger, Confront, 267-268; Th. Darnstädt, Th., M. Rosenbach en G.P. Schmitz, 'Arming for Virtual Battle. The Dangerous New Rules of Cyberwar', SpiegelOnline, 4 april 2013. Vgl. luitenant-generaal Michael Flynn, geciteerd in Bowden, Finish, xii.
62 Sanger, Confront, 265-266.
63 Sanger, Confront, 268-269; Shanker, 'Pentagon'. Zie ook B.D. DeCoster, Crime or War: Cyberspace Law and its Implications for Intelligence, Carlisle Barracks, PA, 2011; M.N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge 2013.
64 Juist het gegeven dat een oorlog met minder slachtoffers de waarschijnlijkheid van oorlog groter maakte was al in de negentiende eeuw reden voor Florence Nightingale om zich te verzetten tegen de oprichting van het Rode Kruis, Ph. Gourevitch, 'Alms Dealers', The New Yorker, 11 oktober 2010,105-106.

FOTO US DEPARTMENT OF DEFENSE

Tot nu toe vonden onder Obama's presidentschap honderden drone-aanvallen plaats, met duizenden doden. Obama heeft als bijnaam 'de drone-president'

maken van *non-lethal* (niet-dodelijke) wapens,[65] als oorlogen exclusief worden uitgevochten tussen robots (als men tenminste een kapotte robot niet dood verklaart) of als daadwerkelijke oorlogen zich uitsluitend in het virtuele domein of met behulp van onbemande ruimteschepen of -projectielen in *outer space* voltrekken.

In mijn opvatting zijn dus zelfs oorlogen zonder fysiek of kinetisch geweld mogelijk, zoals in een cyberwar of in een oorlog die louter gericht is op maatschappelijke verstoring van processen bij de tegenstander, bijvoorbeeld met behulp van *information operations*. Zulk optreden bevindt zich nog steeds binnen de begrenzing die Von Clausewitz aan het begrip oorlog gaf.[66] Deze (bijna) schone oorlogen waren niet het type oorlogen dat Kant voor ogen had. In zijn oorlogen was sprake van zichtbaar fysiek geweld. Oorlogen vonden in zijn tijd plaats tussen staten die elkaar over land of water konden bereiken. Het luchtruim, de kosmische ruimte of *cyberspace* waren hem als oorlogsarena's onbekend.

Juist deze nieuwe strijdtonelen maken het mogelijk om oorlog te onttrekken aan het oog van een burgerij die de staat zou kunnen corrigeren in zijn (militaire) optreden. Of het nu gaat om drone-aanvallen in bijvoorbeeld Pakistan, om cyberwar of om ruimteoorlogen, het zijn, bezien vanuit het Westen, *remote-control* oorlogen met veelal weinig of weinig zichtbare risico's voor de daders.[67] Dit type oorlog is voor velen in het Westen een *phoney war*, een *drôle de guerre*, 'de meest openbare "geheime" oorlog uit de moderne

65 Vergelijk S. Orbons, Non-Lethality in Reality. A Defence Technology Assessment of its Political and Military Potential (diss. UvA), Breda 2012.

66 Maar niet binnen de begrenzingen van het Correlates of War Project, dat een ondergrens hanteerde van 1000 aan het strijdgewoel gerelateerde doden, hetzij voor het gehele conflict, hetzij op jaarbasis, M.R. Sarkees, 'Defining and Categorizing Wars', M.R. Sarkees en F.W. Wayman, Resort to War. A Data Guide to Inter-State, Extra-State, Intra-State, and Non-State Wars, 1816-2007, Washington D.C 2010, 39-73. D. Garrie, 'Cyber Warfare: What Are the Rules?', The Huffington Post, 17 juni 2013 betoogt evenwel dat in het licht van cyberwar er een noodzaak is ontstaan voor een herdefiniëring van het begrip 'oorlog'. Vergelijk Metz en Cuccia, War.

67 Zie Mazzetti, Way, 100

tijd',[68] een oorlog die er is en die er tegelijk niet is, maar waarvan we incidenteel in de vorm van terroristische aanslagen op het thuisfront of in de vorm van computermalheur iets merken.

Oorlog als klein ongemak

Het is klein ongemak, vergelijkbaar met het nagelschaartje of het flesje parfum dat we niet mee aan boord van het vliegtuig mogen nemen, dat ons eraan herinnert dat er een oorlog gaande is. Oorlog is een soort achtergrondruis geworden, zoals muzak in een winkelcentrum, die meestal niet bewust door ons wordt opgemerkt, totdat de muziek even iets schriller klinkt of we bepaalde tonen menen te herkennen. De bevolking in de westerse wereld vindt het goed dat officiële instanties preventieve en offensieve acties uitvoeren in het kader van de cyber-oorlog '*to disrupt, deny, degrade or destroy*',[69] om het handelen van de tegenstander 'onmogelijk te maken',[70] zoals zij er ook meestal schouderophalend aan voorbijgaat dat *drones* in een onverklaarde oorlog met *Hellfire*- of andere raketten slachtoffers maken onder potentiële of werkelijke terroristen, en soms ook onschuldige burgers die zich op de verkeerde plaats bevinden.[71] Intussen heeft in het kader van dit type oorlogen niet alleen een '*policification*' van de strijdkrachten plaats,[72] maar evenzeer een militarisering van de politie.[73] Juist door de trivialisering ervan wordt oorlog 'a state of mind', een geestesgesteldheid, die geleidelijk het hele leven doordringt.[74] Maar door diezelfde lichtvoetigheid wordt het tegelijk ook steeds moeilijker het nieuwe type oorlogen beslissend te beëindigen dan wanneer er grootschalig geweld zou worden ingezet.[75] De eeuwige oorlog is tegelijk triomf en nederlaag van de oorlogvoering.

De risico's van machts- en geweldmonopolies

Kant ging uit van het statenstelsel zoals hij dat kende in 1795, toen er nog sprake leek van machtsevenwicht. Na de ineenstorting van de Sovjet-Unie en het Warschaupact rond 1990 waren de Verenigde Staten de enige overgebleven supermacht in een wereld waarin landen en groepen niet langer verankerd waren door de dichotomie van de Koude Oorlog. Aan militair optreden van de Amerikaanse regering werden vanuit Moskou niet veel restricties meer opgelegd en de Verenigde Staten konden het zich permitteren zich eveneens weinig aan te trekken van de NAVO en de Veiligheidsraad van de VN.[76]

Eenzijdige Amerikaanse avonturen

Van een door het recht of een vredesbond gedragen internationale orde, een van Kants voorwaarden voor vrede, was dus geen sprake. Dit leidde tot een reeks van eenzijdige Amerikaanse avonturen, hoogstens geschraagd door *coalitions of the willing*. In dit uitzonderlijke tijdperk van Amerikaanse dominantie konden de Verenigde Staten nieuwe doctrines en technieken hanteren die zich, wanneer anderen zich deze eigen hebben gemaakt, als een boemerang tegen de 21-ste eeuwse Faust zullen keren en verder bijdragen aan het begrip 'eeuwige oorlog'.[77]

68 Turse en Engelhardt, Planet, 33.

69 J.T. Richelson, 'National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document' - National Security Archive Electronic Briefing Book No. 424, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424 Zie ook T. Eshel, 'Defense White Paper Outlines French Cyberwarfare Priorities', http://defense-update.com/20130504_france_livre_blanc_cybersecurity.html.

70 Jaarverslag Militaire Inlichtingen- en Veiligheidsdienst 2012, 13.

71 Robbins, War, 5; The Bureau of Investigative Journalism, 'Leaked Pakistani report confirms high civilian death toll in CIA drone strikes', http://www.the bureau-investigates.com, 22 juni 2013.

72 R. Crelinsten, Counterterrorism, Cambridge/Malden, MA, 2009, 84.

73 R. Balko, Rise of the Warrior Cop. The Militarization of America's Police Forces. New York 2013; idem, 'Rise of the Warrior Cop', The Wall Street Journal, 25 juli 2013.

74 R.J. González, Militarizing Culture. Essays on the Warfare State, Walnut Creek, CA, 2012; E. Sangster, 'Militarising Education', Open Democracy, 27 november 2012.

75 Vergelijk Sanger, Confront, 244 en 422.

76 R. Kagan, Balans van de macht. De kloof tussen Amerika en Europa, Amsterdam 2003, 59-60 en 96.

77 Scahill, Wars, 520. Over de verspreiding van drones zie K. Roberts, 'When the Whole World Has Drones', National Journal, 23 maart 2013; A. Erickson & A. Strange, 'China Has Drones. Now What?', Foreign Affairs, 23 mei 2013; G. Ingersoll en M. Kelley (2013), 'America Is Setting a Dangerous Precedent for the Drone Age', Business Insider, 9 januari 2013; G. Cohen, 'Defense Minister on Sinai Drone Strike: Israel respects Egypt's sovereignty', Haaretz, 11 augustus 2013; 'German Police Shoot Down Model Plane Terror Plot', SpiegelOnline, 25 juni 2013; J. Kaiman en J. McCurry (2013), 'Japan and China step up drone race as tensions build over disputed islands', The Guardian, 9 januari 2013; J. Michaels, 'Experts: Drones basis for new global arms race', USA Today, 9 januari 2013; Q. Siddique, 'The United States' Drone Program in Pakistan: An Analysis of the Efficacy and the Pakistani Government's Complicity', SISA Report no. 4, 8 april 2013, 8 en 54; Turse en Engelhardt, Planet, 14-015, 31; J. Warrick, 'Russian, Iranian technology is boosting Assad's assault on Syrian rebels', The Washington Post, 2 juni 2013; P. Rogers, 'An asymmetrical drone war', Open Democracy, 19 augustus 2010; idem, 'An arms craze: drones to lasers', Open Democracy, 2 mei 2013; Zenko, Reforming, 17-21.

Deze Amerikaanse *hybris* (overmoed) werd mede mogelijk gemaakt door een unieke en nog steeds voortschrijdende uitbreiding van de macht van de Amerikaanse president op de terreinen van de buitenlandse politiek en oorlogvoering na 9/11 ten koste van het Amerikaanse Congres.[78] Door hun gelijkgestemdheid ten aanzien van de *war on terror* verstrekten de democraten en de republikeinen de president een blanco cheque.[79] In het verleden waren noodbevoegdheden van de president na verloop van tijd weer verdwenen, merkte terrorismedeskundige Brian Jenkins in juni 2013 op: 'Maar we verkeren nu in een situatie [de *war on terror*] die geen definitief einde kent. Als er geen eind is, dan accumuleren deze bevoegdheden en accumuleren en accumuleren. Dit is het fundamentele verschil. Wat we in stelling brengen wordt een permanent onderdeel van het landschap'.[80]

De eeuwige oorlog is tegelijk triomf en nederlaag van de oorlogvoering

Terwijl Kant uitging van republieken van gelijkwaardige staatsburgers met een sterke beleidsinvloed, heeft de Amerikaanse bevolking en haar vertegenwoordigers geen greep meer op het defensiebeleid van de president, voor wie geldt: er zijn strijdkrachten en ze worden gebruikt, punt uit. Zoals de Amerikaanse politiek commentator Rachel Maddow het uitdrukt: 'oorlogvoeren is een vrijwel autonome functie van de Amerikaanse staat geworden. Het stopt nooit.'[81]

Voor zover er sprake is van invloed buiten de sfeer van de uitvoerende macht, komt die van het door Eisenhower al onderkende militair-industriële complex, sinds 9/11 aangevuld met een *intelligence & security*-component.[82] De ontwikkeling van een dergelijk specifiek deelbelang had Kant niet voorzien bij zijn veronderstelling dat de algemene wens naar welvaart zich tegen de oorlog zou keren.

Paradox

Wat Kant wel goed had voorzien, was dat een gewapende burgerij, die slechts voor zelfverdediging in actie zou komen, een betere garantie tegen oorlog was dan een beroepsleger. Dienstplichtigen maken een oorlog zicht- en voelbaarder dan een beroepsleger waarbij de samenleving minder direct betrokken is. Sinds het interbellum hebben er nog nooit zo weinig Amerikanen gediend in de strijdkrachten als de afgelopen jaren. Hoewel de Verenigde Staten de afgelopen tien jaar in twee langdurige oorlogen verwikkeld zijn geweest, geeft de helft van de Amerikaanse bevolking aan zelfs niet marginaal door die oorlogen geraakt te zijn.

Juist omdat de verstoring van het maatschappelijk leven zo gering is geweest, is het gemakkelijker geworden deze fysieke oorlogen te voeren.[83] Dit is dus wederom een paradox: hoe minder militairen, des te meer oorlog.

'Covert wars'

Aan een van allerbelangrijkste voorwaarden van Kant voor eeuwige vrede, non-interventie, is de laatste decennia allerminst voldaan. Ten eerste wordt er in het kader van vredesoperaties ingegrepen in andere landen vanuit de redenering dat een land dat niet kan (of wil) voorzien in de bescherming van essentiële rechten van zijn burgers, zijn recht op soevereiniteit verspeelt. Het verlangen in zo'n geval niet

78 Vergelijk Bowden, Finish, 70; Sanger, Confront, New York 2013, xii en 422; Ch. Savage, Takeover: The Return of the Imperial Presidency and the Subversion of American Democracy, New York 2008; Carter, Violence, 185; Scahill, Wars, xxiii, 9-12, 19-20, 24-25, 175, 352, 354 en 453-454; A. Rosenthal, 'The Forever War', The New York Times, 17 mei 2013; R. Brooks, 'The War Professor. Can Obama finally make the legal case for his war on terror?', Foreign Policy, 23 mei 2013.

79 Robbins, War, 5.

80 Geciteerd in F. Kaplan, '"The Foundation of a Very Oppressive State"', Slate Magazine, 7 juni 2013.

81 Maddow, Drift, 202-203, zie ook ibidem, 7-8, 149, 153-154.

82 Vgl. T. Engelhardt, 'The Enemy-Industrial Complex. How to Turn a World Lacking in Enemies into the Most Threatening Place in the Universe', TomDispatch.com, 14 april 2013, http://www.tomdispatch.com/post/175687/tomgram%3A_engelhardt,_the_cathedral_of_the_enemy; W.M. Arkin, American Coup. Martial Life and the Invisible Sabotage of the Constitution, New York (verschijnt binnenkort).

83 Maddow, Drift, 202.

FOTO US DEPARTMENT OF DEFENSE

'Aanvallen met drones, cyberwar of ruimteoorlogen zijn bezien vanuit het Westen 'remote control' oorlogen met veelal weinig of weinig zichtbare risico's voor de daders.' Op de foto: een Hellfire-raket

te volstaan met het opleggen van een negatieve vrede (het tot zwijgen brengen van wapens), maar invulling te geven aan een positieve vrede[84] draagt bij aan de verlenging van conflicten.

Maar ook buiten het kader van vredesoperaties wordt herhaaldelijk militair geïntervenieerd in andere landen, veelal op weinig transparante wijze. Met zijn kritiek op sluipmoord, gif mengen of het uitlokken van verraad keerde Kant zich juist tegen zogeheten *covert wars*, *covert operations* en *covert acts*, die vaak mede gedragen worden door *intelligence*.

Het onderscheid tussen inlichtingen- en militaire operaties is de laatste jaren steeds verder vervaagd. Het Pentagon en de CIA zijn bijvoorbeeld steeds meer op elkaar gaan lijken. De CIA is een 'moordmachine'[85] geworden en het Pentagon een halve spionageorganisatie, waardoor een dusdanig militair-*intelligence* complex is ontstaan dat er gesproken kan worden van zogeheten *intel wars*.[86]

84 L. May, After War Ends. A Philosophical Perspective, Cambridge 2012.

85 Zie bijv. S. Ackerman, 'How the CIA Became "One Hell of a Killing Machine"', Wired, 9 februari 2011; J. Shashanki, 'America's Killing Spree, The World Today, August and September 2013; T. Harnden, 'Obama in Thrall to CIA Killing Machine', Real Cllear Politics, 16 april 2013; F. Kaplan, 'Killing Machine', The New York Times, 10 mei 2013; D. Bates, 'Post 9/11 CIA has become a killing machine focused on hunting down terrorists "faster than they can grow them"', Mail Online, 2 september 2011; 'America's killing machine', The Economist, 13 april 2013.

86 B.G.J. de Graaff, 'Waterboarding, rendition, secret flights and prisons. Verwording of verwezenlijking van inlichtingenvergaring als methode van terrorismebestrijding aan het begin van de 21e eeuw?', M. Kowalski & M. Meeder (eds.), Contraterrorisme en ethiek, Amsterdam 2011, 18; Maddow, Drift, 198; Mazzetti, Way, 4-5; Aid, Intel Wars; M. Ambinder & D.B. Grady, Deep State. Inside the Government Secrecy Industry, Hoboken, NJ, 2013, 119-120 en 153; Sanger, Confront, 79; J. Warrick, The Triple Agent. The al-Qaeda Mole Who Infiltrated the CIA, New York 2011, 18; Scahill, Wars, 48-60, 93-101, 162, 167-178, 350-351, 353; R. Beckhusen, 'Army Seeks Spy Training for Soldiers', Defense News, 16 april 2013.

Als bindmiddel tussen deze militaire en de *intelligence*-component dienen de snel inzetbare *special operation forces*, waarvan het bedrag op de Amerikaanse begroting in het decennium sinds 9/11 is vervijfvoudigd.[87] Juist het *intelligence*-element heeft vanuit zijn specifieke natuur bijgedragen aan het alomvattende en eindeloze karakter van oorlog. Targets werden steeds meer 'everyone, everywhere' en anders dan reguliere oorlogen eindigt *intelligence* nooit.[88]

De inzet van *drones*, extra-territoriale arrestaties en gevangenhouding, waarbij het ene land willekeurig waar ter wereld dan ook als een vorm van '"pre-crime" justice' ingrijpt,[89] heeft van de slachtoffers een soort negatief gedefinieerde wereldburgers gemaakt.[90] Of zoals Ronald Crelinsten, onderzoeker van het *Centre for Global Studies* van de Canadese Universiteit van Victoria, het formuleerde: 'Het idee dat de militairen van een land iedereen en alles overal in de wereld maar kunnen observeren, afluisteren, vastleggen en naspeuren en naar believen aanvallen met op afstand bestuurde vliegtuigen of wapens vanuit de ruimte is de ultieme geïndividualiseerde wijze van oorlogvoering'.[91]

Tot slot

'Blijvende veiligheid en aanhoudende vrede vereisen geen eeuwige oorlog', verklaarde president Obama bij de aanvaarding van zijn tweede ambtstermijn.[92] Het lijkt een wanhopige poging de realiteit van de eeuwige oorlog, die hij zelf had helpen bevorderen, in overeenstemming te brengen met een Kantiaanse blijvende vrede.

Even scheen de Amerikaanse president zich nog vast te klampen aan het door hemzelf zoekgemaakte idee dat oorlogen altijd gaan over de vrede die erop volgt. Mogelijk was het ook een reactie op kritiek zoals enkele maanden eerder verwoord in de *Washington Post*, waarin Obama werd verweten dat hij het ad hoc karakter van *targeted killings*, geïnitieerd door zijn voorganger, had getransformeerd in een 'contraterrorismestelsel dat een schijnbaar permanente oorlog mogelijk maakte'.[93] Of op de aankondiging van de speciale rapporteur van de Verenigde Naties voor terrorismebestrijding en mensenrechten Ben Emerson in die tijd dat hij een onderzoek zou instellen naar het gebruik van *drones* en *targeted killing* door de VS.

De reden daarvoor was volgens Emerson dat de westerse democratieën inmiddels bezig waren met 'een wereldwijde oorlog tegen een niet aan een staat gebonden vijand, zonder zich geografische restricties of beperkingen in tijdsduur op te leggen.'[94] Zo'n 220 jaar na Kants spraakmakende geschrift kan worden geconcludeerd dat de eeuwige vrede uitsluitend heerst op het kerkhof.* ■

87 R.A. Best & A. Feickert, Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress, Washington D.C. 2009; V.P. Bramble, Covert Action Lead. Central Intelligence Agency or Special Forces, Fort Leavenworth, KS, 2007; R.C. Gross, Different Worlds: Unacknowledged Special Operations and Covert Action, Carlisle Barracks, PA, 2009; L. Robinson, 'The Future of U.S. Special Operations Forces', http://www.cfr.org/national-security-and-defense/future-us-special-operations-forces/p30323; E. Schmitt & T. Shanker, 'A Commander Seeks to Chart a New Path for Special Operations', The New York Times, 1 mei 2013.

88 Sanger, Confront, 256 en 261; Aid, Intel Wars, 6.

89 Scahill, Wars, 352. Zie bijv. ook J. Bravin, The Terror Courts. Rough Justice at Guantanamo Bay, New Haven/London 2013; G.L. Carle, The Interrogator. An Education, New York 2011; Clarke, Enemies, 143-153; S. Grey, Ghost Plane. The Inside Story of the CIA's Secret Rendition Programme, London 2006; Rodriguez, Measures; Ph. Sands, Torture Team. Deception, Cruelty and the Compromise of Law, London 2008; T. Paglen & A.C. Thompson, Torture Taxi. On the Trail of the CIA's Rendition Flights, Cambridge 2007.

90 Zie M.S. Akbar, 'Obama's Forgotten Victims', The New York Times, 22 mei 2013; Roberts, 'World'; Chr. Woods en A.K. Ross, 'Secret Justice. Former British Citizen killed by drone strikes after passports revoked', The Bureau of Investigative Journalism, 27 februari 2013.

91 Crelinsten, Counterterrorism, 77.

92 Geciteerd in Scahill, Wars, 513.

93 G. Miller, 'Plan for Hunting Terrorists Signals U.S. Intends to Keep Adding Names to Kill Lists', Washington Post, 23 oktober 2012.

94 Geciteerd in Scahill, Wars, 520.

* Dit artikel is een bewerking van 'Why Kant is wrong: the World on its way to eternal war', H. Amersfoort, R. Moelker, J. Soeters & D. Verweij (eds), in: 'Moral Resposibility & Military Effectiveness', *NL ARMS 2013*, Asser Press 2013.

Blijven of weggaan

Linda Polman

Aanvallen op buitenwijken van Damascus: eind augustus sprak *Secretary of State* John Kerry er Amerikaanse Congresleden over toe. Hij probeerde daarbij slinks om Artsen zonder Grenzen (AzG/MSF) medeplichtig te maken aan zijn politieke en militaire agenda door te beweren dat 'AzG-medewerkers ter plekke' geconstateerd hadden dat er chemische wapens waren gebruikt en dat dus militair moest worden ingegrepen.
In mei deelde John Kerry nog warme complimentjes uit aan Amerikaanse diplomaten die zich inspanden voor de democratie in Kyrzachstan. Dat land bestaat niet, maar *who cares*?
Echter, in een speech waar mensenlevens van afhangen, zoals een die is bedoeld om het Congres te bewegen een land te bombarderen, hoop je toch dat zo'n man de feiten op een rijtje heeft. Maar nee. Dat AzG 'ter plekke' is, is niet waar. Dat had Kerry kunnen lezen op de AzG-website: 'Due to significant security risks, MSF staff members have not been able to access the facilities.' AzG bevoorraadt slechts ziekenhuizen ter plekke en medewerkers van die ziekenhuizen zeggen 3600 patiënten met neurotoxische symptomen te hebben gezien. Maar: 'MSF can neither scientifically confirm the cause of these symptoms nor establish who is responsible for the attack.' Kerry probeerde AzG te 'misbruiken als substituut voor onafhankelijk wetenschappelijk onderzoek of als rechtvaardiging voor militair ingrijpen' en daar bedankt de organisatie voor.

Anderhalve week eerder moest AzG ook al tegen misbruik in het geweer komen. De organisatie staakte al haar werk in Somalië en dat terwijl de internationale gemeenschap net opgetogen rapporten had doen verschijnen dat er eindelijk weer een stabiele regering zat en het met de veiligheid de goede kant opging. De ervaring van AzG is anders. De artsen konden hun werk sowieso al niet doen zonder de betaalde bescherming van gewapende milities, maar de aanvallen werden desondanks frequenter. Zestien medewerkers werden vermoord, twee ontvoerd en het aantal bedreigingen en berovingen was ontelbaar. De laatste druppel kwam recent: er waren weer twee collega's vermoord. De dader, in december vorig jaar tot dertig jaar gevangenisstraf veroordeeld, liep na drie maanden alweer vrij rond. Het laatste sprankje hoop doofde daarmee. 'De partijen met wie we minimale veiligheid hadden uitonderhandeld, tolereerden de aanvallen en steunden ze soms. Niemand is opgestaan om te zeggen dat het onacceptabel is om artsen en verplegers te bedreigen, ontvoeren en vermoorden,' aldus AzG.
De organisatie zegt er nadrukkelijk bij dat ze met 'partijen in Somalië' niet alleen al-Shabaab bedoelt en ook niet alleen de Somalische regering in Mogadishu, die zich onverschillig over de moorden toonde door de dader vrij te laten. AzG bedoelt iedereén. Van geen enkele partij op welk niveau dan ook verwachten ze nog bescherming: niet van gewapende groepen, niet van clanoudsten en districtsautoriteiten en niet van de *Federal Somali Government*.
De 'gretigheid' waarmee humanitaire hulp wordt misbruikt en gemanipuleerd werd onmiddellijk na de aankondiging van vertrek opnieuw gedemonstreerd. Binnen een dag bestormden lokale al-Shabaab-vertegenwoordigers twee AzG-ziekenhuizen. Ze verjoegen patiënten en namen apparatuur en voorraden in beslag.
De woordvoerder van de Somalische president was er als de kippen bij om rond te toeteren dat 'het MSF-besluit precies is wat al-Shabaab en al-Qaida willen' en of AzG het besluit maar even wilde herzien om met het volk samen te werken. Tegen al-Shabaab dus. Daar past de organisatie voor: 'De Somalische regering probeert wederom ons een politieke en militaire agenda op te dringen.'
Somalië verlaten is 'een van de pijnlijkste besluiten in onze geschiedenis,' zegt AzG. De artsen behandelden circa vijftigduizend mensen per maand, tweeduizend per dag. Vooralsnog neemt niemand ze over.
'Het is een onmogelijke discussie voor een humanitaire organisatie: hoeveel dode medewerkers zijn acceptabel?', zegt AzG-hoofd Arjen Hehenkamp. Maar AzG opent met het vertrekbesluit die discussie tóch. De vraag is of en welke organisatie(s) aan de gesprekstafel gaan aanschuiven. ■

Sociale media en defensie

*Frans Matser – publicist**

Een paar jaar geleden plaatste een zestienjarig Nederlands meisje een filmpje op YouTube. Daarin zong ze – kennelijk heel fraai – een liedje. Binnen enkele weken werd dit filmpje wereldwijd enkele miljoenen keren gedownload en bekeken. Ze ontving uitnodigingen om bij tientallen televisieprogramma's te komen, met grote artiesten op te treden en om in Amerika, met een grote producer, een cd te maken. De rest is geschiedenis. Tegenwoordig is Esmee Denters een internationaal succesvolle zangeres.

De verkiezingsoverwinning van Barack Obama wordt door de meeste analisten verklaard door de voorsprong die de democraten hebben in het gebruik van sociale media. Ze wisten door een uitgekiende strategie en gebruikmakend van Twitter, Facebook, Linkedin en mail, vrijwel elke potentiële kiezer in Amerika in het bezit van een computer, smartphone of tablet digitaal met hun boodschap te bestoken. Kennelijk kun je de machtigste mens van de wereld worden als je handig met sociale media kunt omgaan.
In Groningse plaatsje Haren liep vorig jaar een feest – op Facebook aangekondigd als Project X – gruwelijk uit de hand. Enorme vernielingen worden aangericht door duizenden mensen die uit het niets werden gemobiliseerd via een ogenschijnlijk onschuldige oproep op Facebook.

De conclusie van dit alles is dat de sociale media een steeds belangrijker plaats innemen bij communicatie en zelfs bezig zijn om de traditionele communicatiemiddelen zoals kranten, tijdschriften, radio en tv naar de tweede plaats te dringen. Veel collega's betogen dat we de sociale media meer moeten gebruiken om de boodschap van defensie uit te dragen.

Een paar maanden geleden overkwam mij iets bijzonders. De redactie van *Armex*, het periodiek van de Koninklijke Nederlandse Vereniging Ons Leger, had mij gevraagd een artikel te schrijven over het huidige personeelsbeleid van Defensie. *Armex* is een typische representant van de oude media, passend bij de vereniging. Het is een blad met veel mooie kleurenfoto's en doorgaans wat tijdloze artikelen over defensie. Het heeft een oplage van zo'n 1500 stuks, die ongeveer *fifty-fifty* verdeeld worden over de 'leden' en de 'doelgroep' van de vereniging. Die doelgroep bestaat uit politici, lobbyisten, publicisten, universiteiten en andere plaatsen waar men hoopt mensen op de ouderwetse wijze enthousiast te kunnen maken voor de boodschap van de vereniging. Die luidt globaal: 'een goede defensie is belangrijk voor Nederland.' Of deze aanpak in de huidige tijd nog werkt, mag u zelf beoordelen. Ik verwachtte er verder weinig opwinding van.

Nadat ik mijn artikel had aangeboden aan de redactie waren er enkele collega's die mij vroegen om een exemplaar. Er zijn immers niet veel mensen met een Armex-abonnement. Om niet allerlei losse bestanden naar mensen toe te moeten sturen, besloot ik gebruik te maken mijn blog 'de bezuinigingsgeneraal', waar ik op onregelmatige tijdstippen wel eens een verhaal achterlaat voor de geïnteresseerde lezer (http://bezuinigingsgeneraal.blogspot.com). Op zo'n blog zit een teller waaruit je kunt aflezen hoeveel verschillende mensen de pagina hebben geopend en dat specifieke

* Op deze plaats vindt u afwisselend een bijdrage van Frans Matser en luitenant-kolonel der Mariniers Marcus Houben.

verhaal hebben gelezen. Doorgaans kijken er enige tientallen mensen naar een verhaal, soms wel eens een paar honderd. *That's it*. Maar wat mij nu overkwam was heel bijzonder.

Een aantal collega's deelden spontaan de link naar mijn verhaal op hun Facebook- en Linkedin-pagina's. Binnen vijf uur bleken 2000 mensen mijn blog te hebben gevonden. Veel van die lezers deelden de blog weer op hun *social media* of twitterden er over. Een militaire vakbond deelde het bericht, diverse websites en *chatboxen* plaatsten of noemden de link en binnen 24 uur was het artikel 5000 keer geopend. Na 48 uur stond de teller op 9000 en uiteindelijk waren er binnen drie dagen ruim 12.000 mensen die dit verhaal hebben gelezen. Toen stopte het, even onverwacht als het begonnen was.

Het is een verhaal over het defensiepersoneelsbeleid. Zo'n verhaal heeft een vrij kleine en strak omlijnde doelgroep: defensiemedewerkers en ex-defensiemedewerkers. Dan praat je bij elkaar misschien over 50.000 mensen. Als twintig procent daarvan een verhaal 'actief' opzoekt, dan gaat het kennelijk over iets wat ze nogal bezighoudt. Want anders dan in sommige andere verhalen probeerde ik dit keer niet de lezer met een paar grappen en grollen aan het denken te zetten. Het is een vrij feitelijke opsomming van een aantal personeelsmaatregelen van de afgelopen jaren en een poging te beschrijven wat de (negatieve) gevolgen daarvan kunnen zijn voor de organisatie. In diezelfde drie dagen krijg ik talloze *likes*, adhesiebetuigingen en commentaren, ook per mail. Unaniem is het commentaar dat de (ex)militairen maar ook veel (ex)burgers bij defensie zich hierin herkennen, en dat velen mijn zorg delen. Tot zover een bijzondere ervaring.

De moraal van dit verhaal is dat sociale media een ongelooflijk krachtig en snel instrument zijn om een boodschap te verspreiden. Maar ook dat, als die boodschap een begrensde doelgroep heeft, ze als een strovuur oplaait, om daarna even snel weer uit te doven. Om dat te illustreren verwijs ik naar het initiatief dat een aantal collega's voor de verkiezingen van 2012 nam om defensie 'meer op de kaart te zetten' en vooral te vrijwaren van verdere bezuinigingen. In een poging een burgerinitiatief te ontketenen stelden ze een petitie op 'handen af van Defensie in het belang van de verzorgingsstaat'. Een burgerinitiatief is een manier om een urgent maatschappelijk probleem aan de politiek duidelijk te maken en de politiek te beïnvloeden. Het initiatief haalde de meeste kranten en enkele radio- en tv-rubrieken, en menig collega ondersteunde dit via zijn Facebook- of twitter-*account*.

Maar ook hier was hetzelfde patroon te zien. In de eerste week waren er zo'n 7000 ondertekenaars, daarna doofde het langzaan uit en uiteindelijk bleef de teller na enkele weken op 20.000 steken. Kennelijk is dat het aantal mensen dat zich voor deze materie interesseert. In november 2012 is deze petitie aan de Tweede Kamer aangeboden, waar ze ongetwijfeld in een diepe lade is opgeborgen. Want om als formeel burgerinitiatief in de Kamer besproken te worden zijn 40.000 stemmen nodig. De petitie 'handen af van de homeopathie' (een wetenschappelijk volstrekt onbewezen medische behandelmethode) haalde dit aantal moeiteloos (46.000), maar de defensiepetitie niet, net als trouwens veelzeggende initiatieven als: 'een zebrapad voor Avans' en 'stop de Dolhuysbrug'. U merkt, we bevinden ons met de landsverdediging in goed gezelschap.

De tweede conclusie van dit verhaal is daarom dat er kennelijk in de maatschappij, buiten het militaire wereldje, maar bar weinig mensen zijn die onze zorgen over de staat van defensie delen. Ook het gebruik van sociale media kan daar weinig aan veranderen! Realiteit is dat de meeste mensen in Nederland heel andere zorgen hebben: de waarde van hun huis, hun pensioen, hun werkgelegenheid, de radicale islam, en gaat u zo maar door. Dat hebben we natuurlijk zelf op ons geweten. Samen met de NAVO-partners, hebben we Nederland na de Tweede Wereldoorlog zo veilig gemaakt dat het merendeel van onze landgenoten geen dag meer zonder sociale media kan, maar zich niet kan voorstellen dat Nederland ooit nog een defensieorganisatie nodig heeft. ■

‘Operation Unified Protector’

Lkol J.P. Schouwenaars

Naar aanleiding van het artikel ‘Operation Unified Protector’ (OUP) wil ik graag reageren.[1] Dit wil ik doen vanuit de achtergrond dat ik tijdens de operatie als stafofficier heb gewerkt in het Office of the Political Advisor van zowel het Joint Forces Command Naples als OUP. Ik wil de auteurs danken voor hun zeer omvattende beschrijving van de operatie en op een aantal aspecten ingaan.

Van internationale verontwaardiging tot militair optreden

Ik denk dat het gerechtvaardigd is te veronderstellen dat de internationale druk voornamelijk van Franse zijde is gekomen en zich niet heeft beperkt tot de VN-Veiligheidsraad. Ook binnen de NAVO en de EU heeft Frankrijk stevige druk uitgeoefend op partners om de besluitvorming niet te blokkeren. Uit diverse gesprekken die ik heb gehad met de beide Amerikaanse politiek adviseurs die aan de operatie verbonden waren, is mij gebleken dat de VS enerzijds Frankrijk heeft gesteund, maar anderzijds ook duidelijk een eigen benadering van de Arabische Lente had ten tijde van de start van de operatie.
De Arabische Lente was volgens de Amerikanen een goede ontwikkeling, die op langere termijn positieve effecten zal hebben op de situatie in veel landen in het Midden-Oosten. Hierbij zal moeten worden geaccepteerd dat dit proces een van lange adem is, dat ook veel instabiliteit zal veroorzaken.
De toenmalige regering zag Amerikaanse bemoeienis met de Arabische Lente als een bedreiging voor het fenomeen.
Te veel bemoeienis zou leiden tot een reactie tegen de VS, mogelijk in het hele Midden-Oosten en zou daarmee de Arabische Lente in de kiem smoren. Deze zienswijze lijkt ook van toepassing op de situatie in Syrië.
Het mandaat is mijns inziens iets beperkter dan de auteurs schetsen. Het aangrijpen van grondtroepen was alleen geoorloofd als deze een directe bedreiging vormden voor de veiligheid van burgers. Politiek relevant is te vermelden dat de resolutie de Afrikaanse Unie oproept een actieve rol te spelen.[2] Ik kom hier nog op terug. Niet onvermeld mag blijven dat resolutie UNSCR 1973 ook een wapenembargo mandateert, en dat het maritieme deel van OUP zich daarmee heeft beziggehouden.

OUP: bijdragen van de coalitie ‘à la carte’

De bijdragen van de coalitie waren inderdaad divers en gingen in een aantal gevallen gepaard met *caveats*. Deze caveats hadden een tweeledig effect. De landen die de meeste ISR-middelen ter beschikking stelden hadden niet de bereidheid de inlichtingen die deze middelen genereerden te delen met anderen.
Het (logische?) gevolg was dat er binnen het *targeting*-proces het zogeheten *five eyes only*-beraad ontstond: Canada, Frankrijk, Italië, het VK en de VS. Dit werkte belemmerend en had ook tot gevolg dat veel missies alleen door deze landen konden worden uitgevoerd.

De constatering van de auteurs dat niet iedereen begrip heeft voor de landen die geen offensieve missies tegen gronddoelen mochten uitvoeren, kan ik vanuit mijn ervaring geheel onderschrijven. Het is op zich eenvoudig uit te leggen dat een politiek besluit beperkingen oplegt aan de inzet van militaire middelen. Dat het zelfs zover wordt doorgevoerd dat de Nederlandse KDC-10 alleen maar vliegtuigen mocht bijtanken die werden ingezet voor de *air-to-air-campaign*, is misschien ook nog wel uit te leggen. Maar ondanks deze politieke uitleg ben ik toch geneigd om de vraag of het ook begrépen is, negatief te beantwoorden.

1 L.W.E.M. van Geel, G. de Koster en F.P.B. Osinga. ‘De NAVO tegen Gaddafi. Operation Unified Protector’, in: *Militaire Spectator* 182 (2013) (5) 220-236.

2 Zie: UNSCR 1973, paragraaf 2:2.

OUP: doelbestrijding en de rol van Special Forces
De auteurs geven aan dat, als er in de beginfase meer aanvalsvliegtuigen ter beschikking waren geweest, er effectiever tegen de Libische troepen had kunnen worden opgetreden. Ik zou deze constatering willen nuanceren met de beperking die het mandaat oplegt. Het mandaat gaf aan dat alleen die grondtroepen mochten worden bestreden die een direct gevaar voor de burgerbevolking opleverden.
De auteurs beschrijven in de paragraaf 'De rol van Special Forces' het gevangennemen van Gaddafi en het beëindigen van de luchtsteun. Wat in dit artikel naar mijn idee onderbelicht is, is de beperking die het luchtwapen had in OUP. Tegen het einde van de operatie, met name na de val van Tripoli eind augustus, werd het steeds moeilijker om doelen te vinden die binnen het mandaat pasten en die op adequate wijze door het luchtwapen konden worden bestreden. Het targeting-proces verliep steeds moeizamer en de efficiënte inzet van het luchtwapen om verdere voortgang in de operatie te boeken, kwam steeds meer onder druk te staan. Door het gevangennemen van Gaddafi is de bevolking gelukkig een langer lijden bespaard gebleven.

Politieke aspecten
In de paragraaf 'Het politieke perspectief' gaan de auteurs vooral in op interne NAVO-politieke aspecten van de operatie en de alliantie.
Een aspect dat ik daaraan zou willen toevoegen is de discussie die er binnen de alliantie is gevoerd over het aangaan van deze operatie. Zoals ik al aangaf, heeft de ambitie van met name Frankrijk om deze operatie te starten, de politieke verhoudingen binnen de alliantie beïnvloed. Zoals bekend heeft Duitsland zich geschikt in de ambitie van andere lidstaten om de operatie uit te voeren.
Het voorhanden zijn van een mandaat van de internationale gemeenschap en de druk van de alliantie zelf was in dit geval voldoende. Maar het heeft echter ook, in ieder geval tijdelijk, de onderlinge verhoudingen bekoeld.
Ten slotte zou ik nog enkele internationale politieke aspecten willen belichten. *Operation Unified Protector* heeft ook het beeld van de NAVO in deze arena beïnvloed. Op de eerste plaats wil ik ingaan op de impact die de operatie heeft gehad op de Afrikaanse Unie (AU). Voor de crisis was Libië – lees Gaddafi – financier van 15 procent van het budget van de Afrikaanse Unie, betaalde de contributies van de meeste kleinere Afrikaanse landen en financierde veel (infrastructurele) projecten in Afrika. Toen bleek dat de AU geen actieve rol wilde spelen in de uitvoering van UNSCR 1973, veranderde de perceptie van de AU ten aanzien van het NAVO-optreden:
in Gaddafi verloren zij een goede bondgenoot en een groot investeerder. Dit werkt ook nu nog door in de verhoudingen tussen de AU en de NAVO. De NAVO heeft de tamelijk onbekende *NATO Support to the African Union Mission* in Addis Abebeba in Ethiopië. Deze missie vloeit voort uit de ondersteuning die de NAVO heeft gegeven in het ontplooien van troepen van de AU naar de missie in Soudan in 2006. Inmiddels is deze ondersteuning uitgegroeid tot een missie om de AU niet alleen met strategisch transport te ondersteunen.
Op verzoek van de AU assisteert de NAVO bij de opbouwen van stafcapaciteit in het hoofdkwartier van de AU en bij de *African Standby Forces* (ASF). Het tekenen van een *Technical Agreement* om de relatie tussen de AU en de NAVO formeel vast te leggen, stond in 2011 op het punt te gebeuren. OUP heeft dit vertraagd en tot op heden is het document niet ondertekend.

Toen de crisis zich ontvouwde en duidelijk werd dat de Afrikaanse Unie niet tot het besluit kon komen om de uitvoering van UNSCR 1973 actief te steunen, heeft de Arabische Liga (AL) zich ermee bemoeid. Hoewel de Arabische Liga niet de reputatie heeft zich te mengen in binnenlandse aangelegenheden van lidstaten, werd toch al vrij snel duidelijk dat de AL in dit geval wel besluiten kon nemen.

De AL heeft echter nooit actief bijgedragen. De militaire bijdrage van landen uit het Midden-Oosten bleef beperkt tot Qatar, Saoedi-Arabië en de Verenigde Arabische Emiraten – alle lid van de *Gulf Coordination Council*.
Al deze staten hebben een soennitisch bewind, met als gevolg dat de verhoudingen tussen de soennieten en de sjiieten in de regio verder op scherp zijn gezet. ■

Schrijftalent gezocht!

In deze Militaire Spectator is plaats gemaakt voor twee gastcolumns. M. Schaake gaat in op digitale vrijheid en cybersecurity,terwijl T. Burgers pleit voor een breder debat over de Digital and Robotic Revolution in Military Affairs.
De redactie van de Militaire Spectator daagt ook andere lezers uit om een gastcolumn te schrijven. Het thema is vrij, maar moet passen binnen de formule van het tijdschrift. De boodschap moet relevant zijn voor de lezers. Het moet gaan om een gefundeerde eigen mening, om een logisch opgebouwd betoog en de feiten moeten kloppen en verifieerbaar zijn. Een bijdrage mag maximaal duizend woorden tellen. U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon). De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur

Defensie in een online verbonden wereld

*M. Schaake**

Waar lange tijd het wapenarsenaal en aantal troepen een graadmeter voor de kracht van een leger leek, wordt weerbaarheid tegenwoordig gemeten aan de mate waarin digitale vrijheid, of cyber-security, kan worden gewaarborgd.
Technologie leidt tot nieuwe vragen over vrede, vrijheid en veiligheid, en raakt bijna elk aspect van onze samenleving. Maar de nieuwe digitale realiteit wordt nog te veel in militaire termen benaderd, terwijl een civiele aanpak ook essentieel is. In beleid ontbreken essentiële maatregelen om Europese belangen veilig te stellen. Zo moeten we de hand in Europese boezem steken en ervoor zorgen dat digitale wapens niet zonder controle worden geëxporteerd naar landen die mensenrechten schenden of onze strategische positie willen ondermijnen.

De Amerikaanse minister van Defensie waarschuwde vorig jaar voor een 'cyber-Pearl Harbor' en er wordt steeds vaker gesproken van een cyber-Koude Oorlog, waarbij het epicentrum niet langer in Moskou, maar in Azië ligt. Dergelijke zware metaforen worden regelmatig gebruikt om de omvang van de dreiging van cyber-aanvallen aan te geven. Ook lijken ze bedoeld om de zwaarst mogelijke reactie te legitimeren. Een cyber-wapenwedloop dreigt, terwijl de juridische kaders nog onduidelijk zijn.

Zowel de NAVO als de verschillende lidstaten zoeken naar doctrines waarin het mandaat voor offensieve capaciteit, maar ook cyber-defensie moet passen. Dat is niet eenvoudig. Zo is het heel lastig om met zekerheid vast te stellen wie een cyber-aanval heeft uitgevoerd; een regering, *hackers* of een terroristische organisatie, of via de computers van mensen die niet weten dat hun computer is geïnfecteerd.
Dat maakt het antwoord op de vraag wat een juiste respons zou zijn dan ook niet evident. De NAVO heeft bijvoorbeeld nog niet besloten of artikel 5 van het Verdrag van Washington ook geldt voor cyber-aanvallen. Over de vraag of cyber-aanvallen met kinetische wapens mogen worden beantwoord, is de politieke discussie nog niet eens volwassen. De EU presen-

* De auteur is Europarlementariër voor D66 en lid van de commissie Buitenlandse Zaken en Internationale Handel. Ze schreef de eerste strategie voor digitale vrijheid in het buitenlandbeleid van de EU.

teerde een cyber-security strategie, maar ze ontweek deze cruciale vraag. Hoe preventie eruit ziet en of preventieve aanvallen daarbij passen, is onderwerp van debat en speculatie. Een bekend voorbeeld van zo'n preventieve cyber-aanval was Stuxnet, waarvan men aanneemt dat de VS en Israël via dit virus het Iraanse atoomprogramma aanvielen.

Steeds meer landen hebben een 'elektronisch leger'. In Syrië wordt dat ingezet om dissidenten op te sporen of om de bevolking te onderdrukken, maar ook voor aanvallen op online doelen van tegenstanders. Verschillende westerse media werden door het Syrisch elektronische leger gehackt. In China is online surveillance een bloeiende industrie: honderdduizenden Chinezen verdienen hun brood met het controleren waar hun medemens online gaat en staat. Activistenbewegingen als Anonymous zijn nieuwe spelers op het wereldtoneel, onvoorspelbaar en grillig, maar ze kunnen ook rekenen op een brede maatschappelijke sympathie.

Nieuwe digitale technologieën leiden gelukkig niet alleen tot vragen over veiligheid en defensie, maar zorgen wereldwijd ook voor veranderingen binnen samenlevingen. Veel van die veranderingen zijn positief en gaan over ontwikkeling, individuele vrijheid, ontplooiing, economische kansen, het delen van kennis of het eenvoudiger maken van diensten. Met behulp van nieuwe technologieën is het voor individuen gemakkelijker om hun mensenrechten, zoals vrije expressie of toegang tot informatie, op te eisen. Ook worden met behulp van mobiele telefoons schendingen van mensenrechten vastgelegd en gedeeld. De wereld is met één druk op de knop ooggetuige van oorlogen.
Een constante factor in de discussies over digitale vrijheid en cyber-security is dat de traditionele concepten van jurisdictie, gevestigd in de natiestaat en de zwaardmacht van de staat, niet langer gelden. Grote delen van onze kritieke infrastructuur zijn in private handen. De wederkerige relatie tussen soevereine staten en de online grenzeloosheid leidt zowel tot kansen als bedreigingen. Toch overlappen publieke en private belangen niet altijd.

Waar er enerzijds macht van regeringen naar individuen vloeit, zijn het vooral bedrijven die steeds meer invloed krijgen. Ze hebben een ongekend invloedrijke positie op het internet. In deze verbonden wereld worden bedrijven zelf ook steeds vaker geconfronteerd met vragen die voorheen alleen aan diplomaten of overheden waren voorbehouden. Toen de video *The Innocence of Muslims* in verschillende landen leidde tot gewelddadige demonstraties, vroeg het Witte Huis aan Google om deze video van haar dienst *YouTube* af te halen. Tegelijkertijd wil het Amerikaanse ministerie van Buitenlandse Zaken juist niet dat de digitale vrijheid van mensen wordt beperkt door censuur.

Terwijl de technologie zich razendsnel ontwikkelt, lopen wet- en regelgeving en veiligheidsdoctrines achter. Als die niet worden aangepast aan een online verbonden realiteit, verliezen we relevantie en geloofwaardigheid. Om te beginnen moet de EU-regelgeving over de export van de meest agressieve technologieën worden aangescherpt. Massasurveillance, massacensuur, maar ook hackingtechnologie of kwetsbaarheden in veelgebruikte software worden momenteel zonder toezicht verhandeld. Dat staat in schril contrast met de bescherming die de EU handhaaft als het gaat om producten als speelgoed, voedingsmiddelen en chemicaliën. Het heeft weinig zin om cyber-verdediging te versterken terwijl vijandelijke spelers hun producten kopen van Europese bedrijven. Deze digitale wapenhandel moet stoppen. We moeten dit gat snel dichten en die verantwoordelijkheid ligt niet alleen bij defensie. Politiek leiderschap en maatschappelijke betrokkenheid zijn onmisbaar.

Omdat in principe ieder mens ter wereld nieuwe technologieën kan gebruiken, moet de verdediging van open internet en van kritieke informatie-infrastructuur een gedeelde verantwoordelijkheid zijn van overheid, bedrijfsleven en de maatschappij als geheel. Afspraken over democratische controle moeten helder worden gemaakt. Metaforen over een cyber-Koude Oorlog wekken te gemakkelijk de suggestie dat defensie alléén kan zorgen voor digitale vrede en veiligheid. ■

Meer dan killer robots? Alternatieve toepassingen voor gerobotiseerde (wapen)systemen

T.J. Burgers

Een analyse van zowel het Nederlandse als het internationale debat van het laatste decennium over de *Digital and Robotic Revolution in Military Affairs* (DRRMA), leert dat de discussie gedomineerd wordt door mogelijke offensieve toepassingen van *remotely piloted aircraft* (RPA): gerobotiseerde vliegende (wapen)systemen.
In het bijzonder de inzet van unmanned *combat aerial vehicles* (UCAV's) – onder een breder publiek beter bekend als bewapende *drones* – bepaalt grotendeels de richting van het debat.[1]

Hoewel Israël deze UCAV's al gebruikt heeft bij conflicten, riep de inzet van dergelijke toestellen in de oorlogen in Afghanistan en Irak – waar deze wapensystemen op grote schaal werden ingezet – vragen op over de ethische en juridische implicaties. Het debat werd ook nog eens verhevigd door de controversiële *targeted killing*-campagne van de CIA in Pakistan, Jemen en Somalië, om met gewapende UCAV's mogelijke terroristen uit te schakelen.
Deze aanvallen waren vaak gebaseerd op uiterst minimaal en veelal discutabel verkregen bewijs en vonden plaats buiten elke vorm van internationaal recht.[2] Deze uiterst omstreden campagne domineert sindsdien grotendeels de discussie over de inzet van gerobotiseerde vliegende wapensystemen. Deze eenzijdige focus heeft negatieve implicaties voor het bredere debat over de DRRMA. De controverse over de campagne van de CIA leidt ertoe dat de algemene ontwikkeling van de DRRMA, zoals bijvoorbeeld de inzet van RPA's in conventionele oorlogvoering, met steeds meer scepsis bekeken wordt.
Niet alleen in het publieke debat zijn RPA's inmiddels een controversieel thema, ook onder verantwoordelijke politici en internationale organisaties is vanwege de CIA-campagne een grote scepsis ten opzichte van de DRRMA ontstaan.[3] Hoewel president Obama recentelijk aankondigde de CIA-campagnes te zullen herzien vanwege de maatschappelijke kritiek en omdat er twijfel is over de effectiviteit, kunnen we voorspellen dat de controverse rondom de inzet van (gewapende) RPA's zal aanhouden.
De aanvallen gaan immers nog steeds door en het ziet er zodoende naar uit dat het gewapende RPA de komende tijd het *weapon of choice* voor de Verenigde Staten blijft.[4] Daardoor valt het te betwijfelen of het debat over de ontwik-

1 Ook de term Remotely Piloted Vehicle (RPV) wordt gebruikt. Dit is de officiële term bij de meeste luchtmachten.

2 In het bijzonder de signature strikes, waarin mogelijke doelwitten werden geïdentificeerd en aangevallen na analyse van mogelijke gedragspatronen, leidden tot de nodige controverse omdat de CIA in veel gevallen de definitie voor mogelijke doelwitten bijzonder ruim interpreteerde; elke mannelijke persoon in de leeftijd tussen 18 en 65 in de regio waar al-Qaida en aanverwante organisaties actief zijn is een mogelijk doelwit. Voor een verdere evaluatie van de drone strikes zie: Micah Zenko, Reforming US Drone Strike Policies (Council on Foreign Relations Special Report, No 65).

3 www.ipsnews.net/2013/02/drone-a-dirty-word-in-the-u-n-lexicon.

4 Het spectrum van mogelijkheden die de regering-Obama heeft om terroristische netwerken in Pakistan, Jemen en Somalië te bestrijden is relatief gering. In dit spectrum blijven drones naar alle waarschijnlijkheid het weapon of choice: het (politieke) risico is een stuk lager vergeleken met de inzet van grondtroepen – de andere meest voordehand liggende optie. Daarnaast zijn drones relatief goedkoop en hebben ze de afgelopen jaren hun effectiviteit aangetoond, want al-Qaida is er als organisatie door gedicimeerd. Voor verdere informatie zie ook: www.foreignaffairs.com/articles/139453/daniel-byman/why-drones-work en www.foreignpolicy.com/articles/2013/05/24/indispensible_weapon_drones_obama?page=full.

keling van de DRRMA in de komende maanden en jaren ruimer gevoerd gaat worden. En dat is te betreuren, omdat er wel degelijk alternatieve applicaties van de DRRMA mogelijk zijn en zelfs al gebruikt worden, maar deze blijven onderbelicht in het huidige debat. Nu is bijvoorbeeld de inzet van RPA's voor surveillance en inlichtingen niet nieuw. De Predator – misschien wel de icoon onder de drones – werd voor deze taken al operationeel ingezet in Bosnië in 1995.
Sindsdien zijn drones frequent ingezet – zowel onbewapend als bewapend[5] – maar in bijna alle gevallen ter ondersteuning van conventionele militaire missies.

Het spectrum van mogelijke toepassingen zou echter geografisch, dimensionaal en inhoudelijk verbreed moeten worden. Een goed voorbeeld hiervan is de inzet van de eerste RPA's in de MONUC-missie in Congo en de missies in Tsjaad en Libanon, waar RPA's de potentiële meerwaarde van de inzet van gerobotiseerde systemen in onconventionele (militaire) operaties aantoonden. Verder kunnen gerobotiseerde systemen niet alleen op het gebied van vredesoperaties een 'revolutie' op gang brengen; ook in de humanitaire sector zou dit mogelijk zijn. Want als bijvoorbeeld Amerikaanse mariniers in afgelegen gebieden in Afghanistan logistiek bevoorraad kunnen worden door onbewapende K-MAX robothelikopters, zou dit ook mogelijk moeten zijn voor afgelegen gebieden waar humanitaire organisaties hulp leveren of dat proberen. Helikopter-RPA's zoals de K-MAX zouden uitstekend geschikt zijn voor dergelijke 'dangerous, dirty and by time routine' humanitaire taken. Een bijkomend voordeel is dat er minder levensgevaar dreigt voor bemanningen en dat de inzet van onbemande helikopters economischer lijkt dan de inzet van bemande toestellen. Daarom moeten de academische en militaire gemeenschap hun invloed aanwenden om te zorgen dat het debat in de komende jaren weer verbreed wordt. Mede gelet op hun technologische voorsprong en expertise op dit gebied zouden de Verenigde Naties en ook Europese landen hierin het voortouw kunnen nemen. Mijn inziens levert dit een win-win situatie op waarin westerse landen wederom op grotere schaal betrokken worden bij vredesoperaties en waarin de VN de effectiviteit van haar vredesoperaties zou kunnen vergroten. Het spreekt voor zich dat bovenstaand scenario in een juridisch en ethisch raamwerk ingebed moet worden. De VN zou hiertoe de aanzet kunnen geven in het kader van haar operaties.

Dat RPA's al succesvol logistiek zijn ingezet in de hedendaagse asymmetrische oorlogvoering toont aan dat de potentiële meerwaarde van de DRRMA niet enkel beperkt is tot kinetische taken in een conventionele oorlogvoering.

Het debat over de *digital and robotic revolution in military affairs* moet breder zijn dan alleen de inzet van gewapende drones

Ook op andere gebieden kan de DRRMA voor een 'revolutie' zorgen door alternatieve toepassingen en inzetmogelijkheden. Gezien de duidelijke meerwaarde van zulke alternatieve applicaties is een breder debat niet alleen wenselijk, maar noodzakelijk. Daarom pleit ik voor diepgaand(er) onderzoek naar de alternatieve toepassingen van RPA's en in een breder verband van de DRRMA. Een onderzoek en een debat dat zich niet enkel richt op de CIA-campagnes en *killer robots*, maar waarin alle mogelijke applicaties van *remotely-piloted systems* in alle typen militaire en niet-militaire missies onderzocht worden. Het is duidelijk dat de DRRMA humanitaire meerwaarde heeft en vanuit dat oogpunt de volle aandacht verdient. ■

5 In de oorlog in Afghanistan werden gewapende drones voor het eerst ingezet. Zie ook Frank Morring Jr., 'Blame Game', in: *Aviation Week & Space Technology* (maart 2004).
6 http://articles.washingtonpost.com/2013-01-08/world/36210223_1_laboratory-for-intelligence-devices-surveillance-drones-peacekeeping-missions.
7 Zie: www.washingtontimes.com/news/2013/may/7/us-marines-employ-drone-copters-afghan-war.
8 Idem.

Cyber War Will Not Take Place

Door Thomas Rid
Londen (Hurst & Company) 2013
ISBN 9781849042802
218 blz.
€ 18,-

Sommige titels zijn bedoeld om te prikkelen en maken dat ook waar. *Cyber War Will Not Take Place* van Thomas Rid is voor cyberfanatici bijna een rode lap, een titel die hen uitdaagt het boek op te pakken en schreeuwt om weerlegd te worden. Het boek blijkt echter ook voor niet-insiders zeer lezenswaardig. Onder dezelfde titel publiceerde Rid overigens eerder een artikel in het *Journal of Strategic Studies*,[1] herdrukt in de Nederlandse bundel *Cyber Warfare. Critical Perspectives*.[2] Nu heeft Rid zijn kerngedachten verder uitgewerkt in een boek, waarmee hij tegenwicht wil bieden aan de doemscenario's, misconcepties en *fear mongering* die hij waarneemt bij politici, experts, de industrie en hoge ambtenaren. Kreten als 'digital Pearl Harbor' (Knake 2010, Panetta 2011) en 'Cyberwar is coming' (Rand 1993) vertroebelen namelijk het beeld van beleidsmakers. Rid argumenteert dat het zo'n vaart niet loopt: er heeft nog geen cyberoorlog plaatsgevonden en dat zal ook in de nabije toekomst niet gebeuren.

Gedetailleerd

Rid bouwt zijn argumenten gestructureerd op. Hij start met de verkenning van begrippen, zoals cyberwapens en cyber war. Hierbij hanteert hij een strikte, 'Clausewitziaanse' definitie, waarbij met name het element 'geweld' belangrijk is. Dat heeft in het cyberdomein namelijk een andere invulling en de kans op fysiek geweld is bij cyberaanvallen alleen indirect, door toedoen van het aangevallen informatiesysteem zelf.
De auteur sluit vervolgens een aantal categorieën cyberaanvallen uit van het strikte begrip cyber war: sabotage, spionage en hacktivisme (*subversion*). Van deze categorieën beschrijft hij vlot, maar gedetailleerd, de reikwijdte, aangevuld met veel voorbeelden, uitspraken van belangrijke spelers in dit domein en persoonlijke observaties.
Zijn conclusie is telkens: bij deze categorie is er geen sprake van cyber war, want er zijn geen voorbeelden die als cyberoorlog te kwalificeren zijn.

Theoretisch

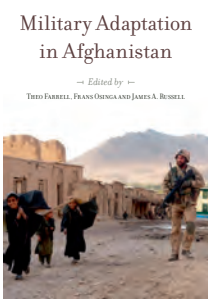
Hier wordt het mij als lezer na enig doordenken overigens te abstract. Het eerst uitzonderen van verschijningsvormen van cyberaanvallen als vorm van cyber war, om daarna te constateren dat het geen cyber war is, is een (te) theoretische exercitie. Een strikte hantering van de definitie is op papier weliswaar mooi, maar verhult dat sabotageacties als Stuxnet wel degelijk een gewelddadig instrument ter voortzetting van de politiek kunnen zijn. De scheidslijn is echter dun en de wereld is sinds Von Clausewitz ook veranderd door technologische ontwikkelingen en geopolitieke verschuivingen. De opvattingen over wat wel en niet (cyber)oorlog is kunnen, gezien werken als *Unrestricted Warfare* van Qiao Liang en Wang Xiangsui uit 1999, dan ook genuanceerder liggen. *Unrestricted Warfare* hanteert bijvoorbeeld een veel breder begrip van oorlogvoering.

Los van deze (ook theoretische) kanttekeningen, is *Cyber War Will Not Take Place* een aangenaam nuchtere en goed geïnformeerde bron over actuele gebeurtenissen en discussies in het cyberdomein. Zonder te vervallen in technisch jargon biedt Rid veel voorbeelden, verbanden en inzichten. Her en der weet Rid de lezer zelfs een glimlach te ontlokken, bijvoorbeeld door Sun Tzu te beschrijven als 'a choppy Twitter feed from 500 BC.' Tijd is kostbaar, dus als er ruimte is voor een boek over de stand van zaken in cyber warfare, dan is dit een prima keus.

Mr. P. de Graaf ■

1 Zie: *Journal of Strategic Studies*, No. 1, February 2012, 5-32.
2 Zie: Paul Ducheine, Frans Osinga, Joseph Soeters (red.), *Cyber Warfare. Critical Perspectives* (Den Haag, Asser Press, 2012).

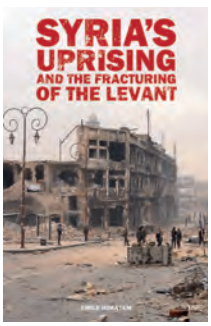
SIGNALERINGEN



Military Adaptation in Afghanistan

Door Theo Farrell, Frans Osinga en James A. Russell (red.)
Palo Alto (Stanford University Press) 2013
368 blz.
ISBN 9780804785891
€ 22,50

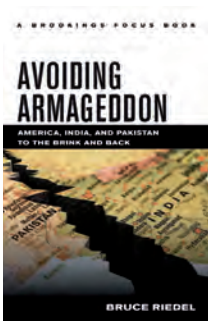
Toen de NAVO in 2003 de leiding kreeg over de *International Security Assistance Force* in Afghanistan, werd de nadruk gelegd op stabilisatie en wederopbouw. Gaandeweg de missie bleken echter ook andere vormen van optreden nodig, zoals militaire steun bij de opbouw van civiel bestuur en nauwe samenwerking met het Afghaanse leger.
In de bundel *Military Adaptation in Afghanistan* analyseren deskundigen hoe krijgsmachten uit drie groepen landen – Groot-Brittannië, Canada, Denemarken, Nederland en de VS; Duitsland en Afghanistan zich aan de ontwikkelingen aanpasten. Over Nederland schreven Martijn Kitzen, Bas Rietjens en Frans Osinga de bijdrage 'Soft Power, the Hard Way: Adaptation by the Netherlands' Task Force Uruzgan'.



Syria's Uprising and the Fracturing of the Levant

Door Emile Hokayem
Londen (International Institute for Strategic Studies–Adelphi series) 2013
212 blz.
ISBN 9780415717380
€ 12,-

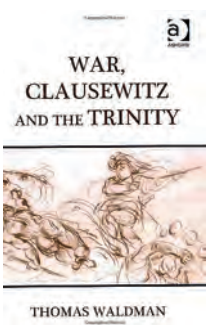
In *Syria's Uprising and the Fracturing of the Levant* analyseert Emile Hokayem, Midden-Oosten deskundige van het *International Institute for Strategic Studies*, hoe het land de afgelopen jaren van een positie als regionale speler is afgegleden naar een burgeroorlog waarbij diverse binnen- en buitenlandse partijen betrokken zijn. Hokayem beschrijft de verschillende oppositiegroepen, maar ook de belangen van het regime van president Assad en zijn 'overlevingsstrategie'. Volgens Hokayem lopen door Syrië regionale 'breuklijnen' die de burgeroorlog verder heeft opengescheurd, met alle politieke en militaire consequenties van dien. Hij gaat in op de belangen van omliggende landen en analyseert ook het debat over westerse hulp aan de rebellen.



Avoiding Armageddon

America, India, and Pakistan to the Brink and Back
Door Bruce Riedel
Washington, D.C. (Brookings Institution Press) 2013
230 blz.
ISBN 9780815724087
€ 21,-

India en Pakistan, twee buurlanden met kernwapens en uiteenlopende culturen en belangen, dreigen de komende jaren instabieler te worden en zullen Zuid-Oost Azië op veiligheidsgebied nog meer gaan domineren. Dat voorspelt voormalig CIA-functionaris Bruce Riedel. Riedel, die de laatste decennia presidenten adviseerde over de regio, zegt dat de Amerikaanse diplomatieke bemoeienis cruciaal is om escalatie tussen Pakistan en India te voorkomen. Wel vindt hij dat de Amerikanen de kwestie-Kashmir te veel uit de weg zijn gegaan en daarin nieuwe initiatieven zouden moeten nemen. Riedel wijst er op dat India en Pakistan veel binnenlandse problemen kennen, waaronder sterke bevolkingsgroei, die op den duur internationaal-politieke gevolgen kunnen hebben.



War, Clausewitz and the Trinity

Door Thomas Waldman
Londen (Ashgate) 2013
216 blz.
ISBN 9781409451396
€ 59,-

Thomas Waldman, als politicoloog verbonden aan de University of York, constateert dat het gedachtegoed van Carl von Clausewitz (1780-1831) vaak wordt aangehaald in strategische studies en militaire geschiedenis. Vaak komen die ideeën echter buiten hun context te liggen en daardoor klopt hun oorspronkelijke betekenis niet meer, stelt Waldman.
Hij probeert *Vom Kriege* van Von Clausewitz opnieuw te interpreteren en gaat daarbij ook in op de drie-eenheid van politiek, krijgsmacht en bevolking, die volgens de Pruisische denker steeds met elkaar verbonden moeten zijn. Waldman is vooral op zoek naar nieuwe perspectieven en haalt elementen uit de theorie van Clausewitz aan waaraan wetenschappers volgens hem voorbij zijn gegaan.

Met dank aan bibliotheek NLDA

ISSN 0026-3869

Mededeling

1995 JRG 164 5

Artikelen uit de *Militaire Spectator* zijn ook te raadplegen via internet.
De artikelen zijn als pdf-bestanden te vinden op www.kvbk-cultureelerfgoed.nl.
Het digitale archief gaat terug tot 1832, het jaar van de oprichting van het tijdschrift en loopt tot en met 2005.

Militaire Spectator

TEKENING: I. KRASSENBURG

WAARIN OPGENOMEN DE OFFICIËLE MEDEDELINGEN VAN DE KONINKLIJKE LANDMACHT EN DE KONINKLIJKE LUCHTMACHT

50 jaar na dato

Themanummer:
De bevrijding van Nederland