Jaargang 186 nummer 4 - 2017

MILITAIRE SPECTATOR

Defensie in het digitale domein

- De Baltische staten, de Russische minderheid en de verdediging van de NAVO
- Technologische innovaties voor de militaire gezondheidszorg

De *Militaire Spectator* digitaal

De *Militaire Spectator* verschijnt ook digitaal met een eigen website. De site www.militairespectator.nl zal uiteindelijk een portal voor de krijgswetenschappen worden.

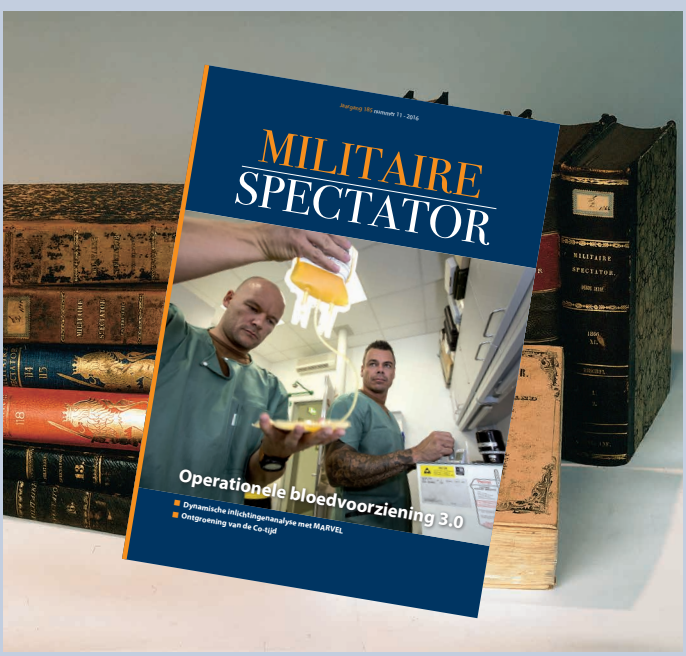
Op de site worden de artikelen, editorialen en columns gemakkelijk toegankelijk gepresenteerd. Ook bevat de site pdf-versies van artikelen uit het gedrukte blad en een digitaal archief van eerder uitgegeven nummers.

Leden van de Koninklijke Vereniging ter Beoefening van de Krijgswetenschap blijven iedere maand een gedrukte versie van de *Militaire Spectator* ontvangen.

Medewerkers van Defensie die de *Militaire Spectator* tot nu toe vanwege hun rang of schaal ontvingen krijgen geen gedrukt exemplaar meer. Zij kunnen zich op de site aanmelden voor de nieuwsbrief en zo op de hoogte blijven van het uitkomen van nieuwe nummers.

De hoofdredacteur

De *Militaire Spectator* is sinds 1832 het militair-wetenschappelijk tijdschrift voor en over de Nederlandse krijgsmacht. Het maakt relevante kennis, wetenschappelijke inzichten, ontwikkelingen en praktijkervaringen toegankelijk en slaat zo een brug tussen theorie en praktijk.
De *Militaire Spectator* stimuleert de gedachtevorming over onderwerpen die de krijgsmacht raken en draagt zodoende bij aan de ontwikkeling van de krijgswetenschap in de breedste zin van het woord.
Op deze wijze geeft het tijdschrift inhoud aan zijn missie: het bijdragen aan de professionalisering van het defensiepersoneel en het verhogen van het kennisniveau van overige geïnteresseerden.
Daarmee bevordert de *Militaire Spectator* ook de dialoog tussen krijgsmacht, wetenschap en samenleving.



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 drs. D. Boissevain
D.Boissevain.01@mindef.nl

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

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: De controlekamer van het Defensie Cyber Commando tijdens een cyberoefening van de NAVO op de Beatrixkazerne in Den Haag, december 2016

Foto MCD, P. Nijhuis

MILITAIRE SPECTATOR

Groeistuipen

Op 14 februari 2017 stelde de minister van Defensie haar lang verwachte visie op de doorontwikkeling van de krijgsmacht bekend aan het parlement.[1] Deze visie moet houvast bieden bij de ontwikkeling van een duurzame, gerede en snel inzetbare krijgsmacht in een onzekere wereld. Niet geheel onterecht wordt opgemerkt dat versterking en vernieuwing van de krijgsmacht hand in hand moeten blijven gaan. De visie bevat geen besluiten; het meerjarig perspectief is immers afhankelijk van toekomstige politieke besluitvorming.
De visie is een goed leesbaar en gestructureerd document. Geheel volgens de militaire traditie volgt het de stappen van het planproces. Op basis van een analyse van mondiale ontwikkelingen en veranderingen in de veiligheidscontext worden keuzes gemaakt over de gewenste ontwikkelingsrichting van de krijgsmacht. Deze richting is vervolgens nader uitgewerkt in zes lijnen van ontwikkeling en geplaatst in een meerjarig perspectief. De laatste lijn van ontwikkeling gaat in op de adaptieve krijgsmacht.
Het concept van de adaptieve krijgsmacht was al eerder bekendgesteld aan het parlement.[2] De adaptieve krijgsmacht richt zich op het vergroten van de flexibiliteit. Daarnaast richt het concept zich op de duurzame samenwerking met andere actoren uit de samenleving, dit alles om de inzetbaarheid en het voortzettingsvermogen van de krijgsmacht te vergroten en het maatschappelijk draagvlak te versterken.
De ontwikkelingslijn van de adaptieve krijgsmacht kent een vrij ambitieuze planning, waarbij allerlei onderwerpen zijn benoemd die de komende jaren de revue zullen passeren. Deze ontwikkelingslijn is geen planmatige blauwdruk, maar slechts richtinggevend.
De personele component is van wezenlijk belang voor het succes van de overige ontwikkelingslijnen. Na jaren van krimp is de organisatie verleerd hoe ze moet omgaan met groei. Voor een bureaucratische organisatie is het gemakkelijker om te krimpen dan om te groeien. Bij krimp zijn er immers vastomlijnde, concrete keuzes te maken die relatief eenvoudig te rechtvaardigen zijn: er is immers geen geld voor. Bij groei gaat het om andere, vaak onzekere keuzes. Wat krijgt de prioriteit en op basis van welke argumenten? Het geld kan maar één keer besteed worden.
Op het eerste gezicht zijn hiermee de twee belangrijkste strategische plannen voor de doorontwikkeling van de krijgsmacht bij elkaar gebracht. Nadere beschouwing geeft echter een ander beeld. De gevolgde strategie voor de omvorming naar een adaptieve krijgsmacht is incrementeel. De ontwikkeling wordt jaarlijks bijgesteld op basis van de kansen en bedreigingen die zich in de omgeving voordoen. Het is een strategie met een opportunistisch element, wat de nodige flexibiliteit met zich meebrengt. Een benadering die goed toepasbaar is in een onzekere omgeving. De strategie voor de overige ontwikkelingslijnen uit het visiedocument is daarentegen formeel en planmatig. De strategie is hierbij uitgewerkt als een gestructureerd *campaign plan*. En daar wringt de schoen. Beide strategische perspectieven zijn elkaars tegenovergestelde. Beide perspectieven hebben voor- en nadelen en kunnen beschouwd worden als een paradox.[3]
Voor een succesvolle implementatie van de ontwikkelingslijnen moeten beide benaderingen goed op elkaar worden afgestemd. Hiervoor zal de strategie voor de ontwikkeling van de adaptieve krijgsmacht wellicht meer moeten opschuiven naar de kant van de meer formele

1 *Houvast in een onzekere wereld*, Kamerbrief minister van Defensie (14 februari 2017).
2 *Plan van aanpak uitvoering Total Force concept*, Kamerbrief ministerie van Defensie (13 januari 2017).
3 Bob de Wit en Ron Meyer, *Strategy Synthesis. Managing Strategy Paradoxes to Create Competitive Advantage* (Andover, Cengage Learning EMEA, vierde editie, 2014).

planmatige benadering. Aan de andere kant zal de strategie voor de doorontwikkeling van de krijgsmacht ook ruimte moeten bieden aan een meer incrementele, op kansen gerichte, benadering.
Gezien de hoge mate van onzekerheid over de ontwikkelingen in de toekomst, moet Defensie er nu voor waken te verzanden in langdurige bureaucratische planprocessen, juist om flexibiliteit te behouden. Flexibiliteit is immers nodig om daadkrachtig te zijn in de doorontwikkeling. Want wie kan de toekomst voorspellen? Wat wordt uiteindelijk het budget van Defensie en voor hoe lang kan Defensie hiervan profiteren? Per slot van rekening had Defensie slechts vier jaar geleden nog een aanzienlijke bezuiniging te verwerken. Is de wereld in vier jaar tijd daadwerkelijk ingrijpend veranderd, of heeft Defensie even de wind mee? Enige terughoudendheid bij de jubelstemming over meer budget is dan ook niet onterecht. Resultaten uit het verleden zijn geen garantie voor de toekomst; zij nopen wel tot enige voorzichtigheid.
In een dynamische, onzekere omgeving is een incrementele strategie per definitie beter in staat om in te spelen op de kansen en bedreigingen die zich in de loop van de tijd voordoen. Een dergelijke strategie is echter wezensvreemd voor de planners binnen de overheid. Het is immers een benadering die met een zeker opportunisme omgaat met de kansen die zich in de toekomst voordoen. Een benadering die in haar zuiverste vorm niet toepasbaar is in de gepolitiseerde wereld van Defensie. Toch zijn elementen van een dergelijke strategie bij nadere beschouwing nog niet zo gek.
Het zal niet verbazen als Defensie binnenkort een ferme projectorganisatie instelt met aan het hoofd een opperofficier om leiding te geven aan de doorontwikkeling van de krijgsmacht. Het zal geen gemakkelijke opdracht zijn. Het eerste dilemma dat zich aftekent is dat Defensie op voorhand moet gaan investeren in wervings- en verwervingscapaciteit om slagvaardig te kunnen optreden. Wervingscapaciteit is nodig om vroegtijdig het juiste personeel aan te trekken, verwervingscapaciteit om de aanbestedingen daadwerkelijk te kunnen realiseren, om echt te kunnen investeren in vernieuwing en verbreding van de krijgsmacht. Hiervoor moet vooruitgelopen worden op de politieke besluitvorming en dat vraagt bestuurlijke stuurmanskunst en pionierswerk. Deze uitdaging moet wel worden aangegaan. Het is immers onverteerbaar als Defensie niet in staat mocht blijken het extra geld om te zetten in investeringen vanwege aanbestedingsperikelen. Onderbesteding is in deze uit den boze: een dergelijke groeistuip zal niet begrepen worden.
Daarnaast zal de projectleider veel aandacht moeten besteden aan de personele component. Groei brengt nieuwe activiteiten met zich mee, wat zal leiden tot een extra beroep op het personeel, gericht op flexibiliteit en vertrouwen in de toekomst. Dit heeft de defensiemedewerker al vele malen eerder gehoord, maar dan in de context van bezuinigingen. Het personeel is het zo langzamerhand beu om te horen dat het morgen allemaal beter wordt. Ondertussen trekt de economie aan en stijgen de verloopcijfers angstwekkend. Tijdens de zoektocht naar flexibel arbeidspotentieel in het kader van de adaptieve krijgsmacht mag het zittende personeel dan ook niet vergeten worden. Nieuw personeel moet worden opgeleid en de mogelijkheid krijgen om kennis en ervaring op te doen en dat vraagt veel van het zittende personeel. Defensie zal nog veel werk moeten verzetten voordat ze geloofwaardig en gecontroleerd kan uitgroeien tot een ware adaptieve, duurzaam gerede en snel inzetbare krijgsmacht. Daarbij kan zij niet te lang vasthouden aan methodes en werkwijzen die de organisatie gewend was toe te passen in tijden van krimp. De organisatie zal ondernemerschap moeten tonen en de kansen moeten grijpen die zich voordoen. Zij moet er wel voor waken dat de botten niet sneller groeien dan het lichaam, anders ontstaan er onherroepelijk groeistuipen. En dat wil niemand. ■

Defensie in het digitale domein

'In de loop van 2017 is het Defensie Cyber Commando operationeel', aldus de commandant, brigade-generaal Hans Folmer.[1] 'Rusland vreest cyberaanval vanuit Nederland', kopte het AD een dag later over een echt incident, een criminele actie waarbij in Nederland geplaatste dataservers een rol zouden spelen.[2] Gelukkig staan beide berichten los van elkaar. Het eerste betreft operationele militaire capaciteit van de Commandant der Strijdkrachten. Het tweede gaat over criminele activiteit. Ze hebben slechts gemeen dat ze zich in het digitale domein afspelen. Voor het aanpakken van dit soort bedreigingen kijken maatschappij en samenleving verwachtingsvol naar Defensie. Dit artikel onderzoekt aan de hand van beleidsontwikkeling welke rollen Defensie in dit digitale domein speelt.

*Prof. dr. P.A.L. Ducheine, brigade-generaal van de Militair Juridische Dienst**

Operaties in dit digitale domein of cyberspace staan in Nederland sinds 2009 op de politieke én militaire agenda.[3] Anno 2015 uit zich dat onder meer in beleidsvisies, zoals de eerste Nationale Cybersecurity Strategie (2011), diens opvolger (2013), in de Defensie Cyber Strategie (2012) en diens actualisering (2015). Een aantal organisaties, hoewel jong, is voor de insiders inmiddels bekend: bijvoorbeeld het Nationale Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, het Defensie Cyber Commando (DCC) en de *Joint Sigint Cyber Unit* van de AIVD en MIVD.

Waar terughoudendheid in defensie-investeringen en inzet in het hoge deel van het geweldsspectrum na 'Afghanistan' de boventoon voerde,[4] is de politieke (en parlementaire) bereidheid te investeren in cybercapaciteiten en daadwerkelijk inzet te overwegen opmerkelijk. Sterker nog: maatschappij en bedrijfsleven kijken vragend naar Defensie voor het aanpakken van bedreigingen in cyberspace.[5] De vraag rijst dan welke rollen Defensie in dit domein speelt.

Ik beoog met dit artikel die vraag te beantwoorden door de beleidsontwikkeling in dit digitale domein te herleiden. De start ligt bij de motie-Knops. Vervolgens wordt de digitale dreiging bezien en het multidisciplinaire antwoord daarop. Dit mondt uit in de eerste Nationale Cyber Security Strategie. De aanloop naar, en

* De auteur dankt drs. Piet Kamphuis, brigade-generaal ir. Hans Folmer en drs. Matthijs Veenendaal voor hun suggesties en commentaar.

1 Interview NOS Journaal vanwege de NAVO-oefening Cyber Coalition, 1-12-2016.

2 AD, 2-12-2016, < http://www.ad.nl/buitenland/rusland-vreest-cyberaanval-vanuit-nederland~ae0f49b8/>.

3 Vijfde dimensie naast land, water, lucht en ruimte ('space'). Zie M.A.D. Tettero & P. de Graaf, 'Het vijfde domein voor de krijgsmacht', in: *Militaire Spectator* 179 (2010) (5) 240-248. Zie voor een oudere agendering: NL ARMS 1999, *Information Operations*, J.M.J. Bosch, H.A.M. Luiijf & A.R. Mollema (red.).

4 Met uitzondering van de luchtmachtbijdrage aan de strijd tegen ISIS.

5 Dennis Broeders, *Investigating the place and role of the armed forces in Dutch cyber security governance*, Department of Sociology, Erasmus University Rotterdam (2014). Zie ook Kamerstukken II 2013–2014, 33 321, nr. 4.

FOTO MCD, P. NIJHUIS

Het Defensie Cyber Commando (DCC) is inmiddels een bekende speler in het digitale domein, samen met het Nationale Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, en de Joint Sigint Cyber Unit van de AIVD en MIVD

de inhoud van de Defensie Cyber Strategie en de actualisering daarvan komen daarna aan de orde. Een reflectie op vitale belangen en een korte blik in de toekomst sluiten dit artikel af.

Parlementaire pressie

CDA-kamerlid Raymond Knops vroeg (tijdens de behandeling van de defensiebegroting op 3 december 2009) de regering via een motie 'in interdepartementaal verband een *cybersecurity* strategie te ontwikkelen' en 'actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO'.[6]

Oud-officier Knops had zich laten leiden door de bedreiging die het toenemende aantal 'cyberaanvallen op computersystemen en netwerken' vormde. De verantwoordelijken daarvoor moesten gezocht worden in kringen van georganiseerde criminaliteit, terreurgroepen en krijgsmachten. Bovendien signaleerde hij dat 'diverse NAVO-landen speciale afdelingen opgericht hebben voor digitale oorlogsvoering [...] en daarbij ook offensieve capaciteiten ontwikkelen'. Hij stelde vast dat cyberwarfare in de Defensiebegroting 2010 ontbrak. In het Kamerdebat wees Knops expliciet naar een incident uit 2007, waarbij Estland digitale verstoringen (vanuit 'het assertieve' Rusland) moest incasseren.[7]

6 Motie-Knops, Voordewind, Eijsink: *Kamerstukken* II 2009/10, 32 123 X, nr. 66. Voortgang in 32 123 X, nr. 89; 26 643, nr. 149 en 164.

7 *Handelingen II* 2009-2010, 32-3020 (2 december 2009). Over dit incident: S.W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford: OUP, 2009, 3-6.

FOTO ANP, M. BEEKMAN

De start van de beleidsontwikkeling in het digitale domein ligt bij de motie-Knops. Oud-officier Knops vroeg aandacht voor de gedachtevorming over cyberwarfare binnen de NAVO

Een jaar later, op 14 december 2010, drong PVV-kamerlid en oud-officier Marcial Hernandez, gesteund door Knops, bij de regering aan 'met een visie te komen over de aanpak van cybercrime/cyberwarfare' waarin het ministerie van Defensie leidend zou moeten zijn.[8] Dit zou tot uitdrukking moeten komen in de inmiddels toegezegde beleidsvisie.

Krijgstaal en dreiging

Hernandez en Knops stonden niet alléén in het samenvoegen van de fenomenen cybercrime en cyberwarfare. Nog steeds leeft bij media en samenleving het idee dat deze twee fenomenen in elkaars verlengde liggen. Op zich is dat opmerkelijk: bankovervallen en het gewapende conflict tussen Oekraïne en Rusland in één adem noemen is immers in fysieke zin bepaald niet gebruikelijk. Terwijl in de digitale wereld martiale termen als 'cyberwarfare' en 'cyberattacks' veelvuldig criminele activiteiten, spionage en allerhande beveiligingsincidenten betreffen.

Sterker nog, een ordinaire diefstal van bedrijfsgegevens zou volgens menigeen aanleiding voor het opwerpen van militaire verdedigingslinies en zelfs een reactie met (digitale) middelen tot gevolg moeten hebben.[9] Dit soort uitspraken getuigt van een krijgshaftige inborst, die het milde militaire karakter van de Nederlandse samenleving miskent. Zelfs wetenschappers die waarschuwen voor een 'militarisering van cyberspace en cybersecurity' vertonen deze neiging tot overreactie.[10]

Diverse bedreigingen

Dat de bedreigingen in cyberspace divers zijn, werd duidelijk in november 2010 met het verschijnen van het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.[11] Anders dan het populaire taalgebruik suggereert, blijkt dan al dat de omvangrijkste bedreigingen geen relatie hebben met oorlogvoering maar met veiligheidsbewustzijn, criminaliteit en spionage.

Ook latere vervolgrapportages vanuit het Nationale Cyber Security Centrum (NCSC), zoals het Cyber Security Beeld Nederland (CSBN), tonen dit beeld.[12]

Toenemende afhankelijkheid van ICT

Het Trendrapport en de CSBN-rapporten benadrukken de toenemende afhankelijkheid van onze economie, maatschappij, bedrijven en burgers van het digitale domein. Dit domein biedt door de ontwikkelingen in de informatie- en communicatietechnologie (ICT) niet slechts ruimte voor zelfontplooiing en het benutten van grondrechten, voor onderwijs en commercie. Door de kwetsbaarheid en afhankelijkheid van digitale netwerken en systemen bevat het ook bedreigingen.

Anders gezegd: de technologische ontwikkeling leidt tot een verandering in menselijk gedrag en verstoringen in technische sfeer raken de mens, maatschappij en bedrijfsleven steeds meer. Niet alleen (individuele en collectieve)

8 Zie ook de motie-Hernandez, *Kamerstukken* II 2010/11, 32 500X, nr. 76.

9 Tijdens het Rondetafelgesprek Digitale oorlogvoering (20 maart 2014) voor de Vaste Kamercommissie van Defensie en Buitenlandse Zaken was dit een van de vragen van Kamerleden. Zie bijvoorbeeld de publieke reactie op de Sony-hack in de VS, 2014.

10 Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet*, Tilburg: De Wereld, 2013.

11 *Kamerstukken* II 2010/11, 28 684, nr. 292: de ministers van Veiligheid & Justitie; Economische Zaken, Landbouw & Innovatie; en Defensie. Het Trendrapport is als bijlage bij dit kamerstuk opgenomen.

12 NCSC (2011) Cybersecurity Beeld Nederland 2011, CSBN-2 (2012), CSBN-3 (2013) en CSBN-4 (2014), via: < https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten>.

wenselijke kansen dienen zich aan, ook ongewenste negatieve kanten komen nadrukkelijk in beeld. De veiligheid in en van het digitale domein komt door malafide activiteiten of neveneffecten onder druk te staan. Digitale veiligheid, veiligheid in het digitale domein of cybersecurity, is in het Trendrapport gedefinieerd als 'een betrouwbare en veilige ICT-omgeving: voorkomen en bestrijden van misbruik en het herstel ervan'.[13]

Wake-up call

Naast de eerder genoemde criminaliteit en spionage leent cyberspace zich (uitstekend) voor subversie, sabotage, activisme en conflictueuze activiteiten die (soms) verband houden met rebellie, opstand, burgeroorlog en interstatelijke gewapende conflicten. Kortom: digitale dreiging in verschillende soorten en maten. Voor Europa en de NAVO dienden de op zichzelf staande digitale verstoringen in Estland (2007) als *wake-up call*.[14] Het Russisch-Georgisch conflict (2008) toont digitale niet-statelijke en patriottische Russische activiteiten die parallel lopen met de militaire fysieke acties.[15]

Digitale onveiligheid is een extreem heterogeen begrip. De omvangrijkste bedreigingen hebben geen relatie hebben met oorlogvoering maar met veiligheidsbewustzijn, criminaliteit en spionage

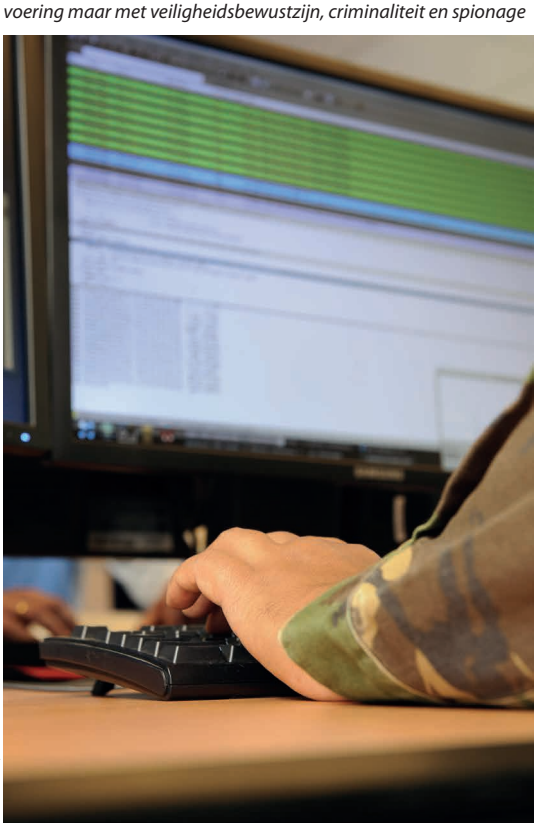


FOTO MCD, H. LEBBE

De ontdekking van Stuxnet trok wereldwijde aandacht als alternatief voor fysieke actie.[16] De uitgekiende *malware*, door de VS en Israël ontwikkeld, beoogde Iraans nucleaire productie te verstoren, het verrijkingsproces te vertragen en een fysieke interventie tegen dat programma uit te stellen, aldus David Sanger.[17]

Multidimensionale dreiging en een multidisciplinaire reactie

Digitale onveiligheid is een extreem heterogeen begrip. Bedreigingen verschillen qua aard en/of intentie. Digitale onveiligheid betreft (een combinatie van) ideologische, criminele, financiële, politieke, economische en militaire inbreuken.[18] Daarachter gaan zowel statelijke als niet-statelijke actoren schuil. Die laatste categorie omvat onder meer (combinaties van) criminelen, activisten, actiegroepen, terroristen, rebellen én commerciële bedrijven.

Een complicerende factor is het feit dat slachtoffers cyberinbreuken niet altijd openlijk delen (voor zover deze überhaupt bekend zijn bij de getroffen organisatie). Geconstateerde inbreuken zijn bovendien niet altijd – technisch of anderszins – te herleiden tot een 'auteur' van die inbreuk.[19]

13 Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010, *Kamerstukken* II 2010/11, 28 684, nr. 292 bijlage, 2.

14 Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: CCDCOE 2010) 15 e.v.

15 Tikk, Kaska & Vihul, 66 e.v..

16 NRC Handelsblad, 16-11-2010, *Kernreactors Iran mogelijk doelwit Stuxnet-worm*, <beta.nrc.nl/nieuws/2010/11/16/kernreactors-iran-doelwit-stuxnet-worm/>, benaderd: 9-12-2010; New York Times, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*: 15 january 2011, <www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>, benaderd: 19-1-2011.

17 David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown 2012) 188 e.v..

18 Tettero & De Graaf, 242.

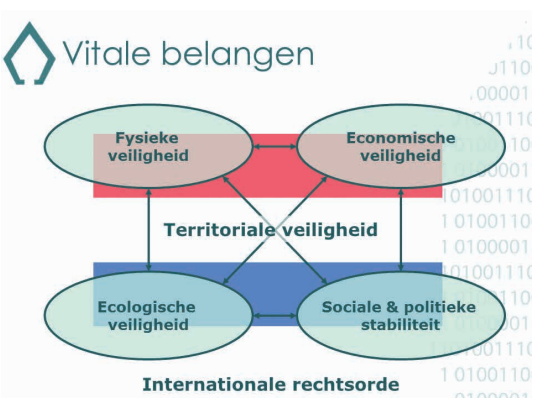
19 Auteur: diegene aan wie de actie wordt toegeschreven of toegedicht. Bijvoorbeeld de dader of de aanvaller.

Vitale belangen

Zo'n veelzijdig en divers dreigingsbeeld vraagt om een multidisciplinaire en getrapte reactie.[20] Uitgangspunt voor veiligheidszorg is de definiëring van 'vitale belangen' zoals dit in de periode 2005-2007 werd gezien:[21]

Vitaal belang: belang dat bepalend is voor de instandhouding van de territoriale, fysieke, economische, ecologische veiligheid en voor de politiek en sociale stabiliteit en maakt dat door het deels of geheel verstoord raken of wegvallen van dat belang het functioneren van de staat en de samenleving in potentie of feitelijk in gevaar komt.[22]

In combinatie met de Internationale Veiligheidsstrategie uit 2013,[23] die naast territoriale en economische veiligheid ook de internationale rechtsorde als een Nederlands vitaal belang aanmerkt, levert dit zes vitale belangen op (zie figuur 1).[24]



Figuur 1 Nationale vitale belangen[25]

De Nederlandse Staat en de Nederlandse overheid staan (uiteindelijk) voor de klassieke taak Nederlands vitale belangen te beschermen en te borgen, ook in het digitale domein. Dat de vitale sectoren doorsneden zijn met digitale systemen, en dat deze zelf veelal ook als vitaal aangemerkt zijn (bijvoorbeeld telecommunicatie), mag helder zijn.

Gelaagde veiligheidsstructuur

De getrapte reactie is bekend van het Stelsel Bewaken en Beveiligen, waarin veiligheidszorg volgens een 'getrapt' systeem is belegd bij
a. private partijen en burgers ('het slot op de deur');
b. decentrale overheden;
c. de rijksoverheid.

Uitgangspunt van het nieuwe stelsel is dat de *verantwoordelijkheid voor de eigen veiligheid primair ligt bij de burger zelf, de organisatie waartoe deze behoort (zoals het bedrijf waar hij werkzaam is) en het decentrale gezag. In aanvulling daarop is er sprake van een bijzondere verantwoordelijkheid van de Rijksoverheid voor een bepaalde groep personen, objecten en diensten.*[26]

Het programma 'bescherming van de vitale infrastructuur' en de Nationale Veiligheidsstrategie (2006-2007) hanteren die gelaagde veiligheidsstructuur eveneens.

De vraag is uiteraard hoe de regering deze digitale veiligheid getrapt en multidisciplinair gaat verzorgen.

Nationale Cybersecurity Strategie 1

Die visie op digitale veiligheid, de *Nationale Cybersecurity Strategie* (NCSS-1) werd op 22 februari 2011 aan de Tweede Kamer aangeboden.[27] Het integrale karakter kwam tot uitdrukking in de ondertitel 'Slagkracht door samenwerking' en de gezamenlijke aanbieding door de ministers van Veiligheid & Justitie, Economische Zaken, Landbouw en Innovatie, Defensie en Binnenlandse Zaken en Koninkrijksrelaties. De door Hernandez en Knops voorgestane alomvattende rol van Defensie kwam daarbij overigens niet tot stand: de coördinerende rol bij kwam bij V&J te liggen.

20 P.A.L. Ducheine, 'Legal Framework for Military Cyber Operations', *Militair Rechtelijk Tijdschrift*, 2013, 106 (1), 9-19, 12.
21 *Kamerstukken* II 2004/05, 26 643, nr. 75, 1, Beleidsbrief Bescherming Vitale Infrastructuur.
22 *Kamerstukken* II 2006/07, 30 821, nr. 2, 3.
23 *Kamerstukken* II 2012-13, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland.
24 Zie HCSS, The Hague Centre for Strategic Studies, *Defensie in het stemhokje*, 1: 'Nederland is een handelsland. Een stabiel internationaal systeem, waarin vrede, veiligheid en vrijhandel prevaleren, is van levensbelang', 2012.
25 Ducheine, P.A.L. *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme.* Nijmegen: Wolf Legal Publishers (diss. UvA), 2008, 20.
26 *Kamerstukken* II, 2002/03, 28 974, nr. 2, 1.
27 *Kamerstukken* II, 2010/11, 26 643, nr. 174.

Nederlands ambitie, zo blijkt uit de NCSS-1, is 'uit te groeien tot de "Digital Gateway to Europe".[28] Het doel is 'het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen.'[29]

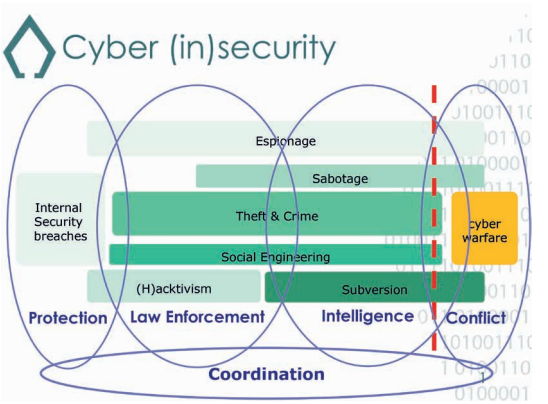
Zes actielijnen moeten dit doel binnen bereik brengen:
- integrale aanpak door publieke en private partijen;
- adequate en actuele dreiging- en risico-analyses;
- weerbaarheid tegen ICT-verstoringen en cyberaanvallen;
- responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
- opsporing en vervolging van cybercrime;
- onderzoek en onderwijs.

Uitgangspunten

Bij de uitwerking van doel en ambitie staan zes uitgangspunten centraal: verbinden en versterken van initiatieven; publiek-private samenwerking; eigen verantwoordelijkheid; actieve internationale samenwerking; proportionaliteit van maatregelen; zelfregulering als het kan, wet- en regelgeving als het moet.[30] In deze uitgangspunten klinkt zowel de democratische rechtsstaat, de Nederlandse staatsstructuur, als de technische en maatschappelijke realiteit door: infrastructuur is immers vaak in private handen en departementen delen verantwoordelijkheid in dit multidimensionale domein.

De strategie voorziet in de oprichting van een 'spin in het web': het Nationale Cyber Security Centrum (NCSC). Het NCSC, waarin het bestaande *Governmental Computer Emergency Response Team* (GovCERT) was opgenomen,[31] is ondergebracht bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het NCSC treedt coördinerend op bij cybersecurity-incidenten die tot overheidshandelen nopen.

Een alternatieve oplossing zou een nieuwe organisatie met eigen bevoegdheden zijn geweest, die tegen een breed spectrum – van 'scriptkiddies', hacktivisme, spionage,



Figuur 2 Digitale dreigingen en security paradigma's

subversie, sabotage, criminaliteit tot cyber-aanvallen met fysieke consequenties – aangewend kan worden.

Duidelijk is dat de organisatie van cybersecurity een klassiek bestuurskundig, (bureau)politiek en organisatiekundig probleem oplevert omdat coördinatie tussen de verschillende onderdelen vereist is.[32] Als gevolg daarvan ontstaan uiteraard ook staatsrechtelijke keuzemomenten (of problemen) die (nader) opgelost zullen moeten worden. De vraag is of oplossingen voor fysieke veiligheidsproblemen onverkort zijn toe te passen op en in het digitale domein.[33]

Private partijen

Naast de overheid is er ook een grote rol weggelegd voor particulieren en private partijen.[34] Dat heeft onder meer te maken met

28 NCSS-1, 3.
29 NCSS-1, 7.
30 NCSS-1, 5-6.
31 GovCERT diende ter bescherming van overheidsnetwerken tegen digitale dreigingen.
32 Zie bijvoorbeeld Muller, E.R., Rogier, L.J.J., Kummeling, H.R.B.M., Dammen, R., Bron, R.P., Woltjer, A.J.Th., & Klakhoven, V.C. *Bestuur, recht en veiligheid. Bestuursrechtelijke bevoegdheden voor openbare ordehandhaving en terrorismebestrijding*. Den Haag: Kluwer Juridische uitgevers, 2008; en Brainich von Brainich Felth, E.T. *Het systeem van crisisbeheersing; bevoegdheden en verplichtingen bij de voorbereiding op en het optreden tijdens crises*. Den Haag: Boom, 2004.
33 Zie bijvoorbeeld Ronald Prins (CEO FOX-IT): 'Een veilige cyberwereld vraagt nieuw denken', in: 38 *Justitiële verkenningen*, No. 1, 40-51, 44.
34 Naast de eigen verantwoordelijkheid in beveiliging die eenieder speelt (het slot op de deur). In cyber is eenieder bijvoorbeeld (mede)verantwoordelijk voor spamfilters, firewall, virusscanners, sterke wachtwoorden, et cetera.

de aard van internet, dat niet vanuit staten en overheden wordt 'bestuurd'. Veel van die private partijen zijn internationaal georganiseerd. Bovendien is een groot deel van de (vitale) digitale infrastructuur in private handen. Het is dan ook begrijpelijk dat de overheid publiek-private samenwerking (en partnership) in het digitale domein propageert. De strategie maakt verder duidelijk dat cybercriminaliteit en cyberwarfare (als bedreiging) slechts facetten zijn van het meer omvattende begrip 'cybersecurity'. Cybersecurity is in de NCSS-1 nog gedefinieerd als:

het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.[35]

Deze idealistische en absoluut geformuleerde 'resultaatsverplichting' zal in NCSS-2 worden omgezet in een realistische en relatief verwoorde 'inspanningsverplichting'. Samen met het Trendrapport en het Cybersecuritybeeld Nederland (2011) valt de overheidsinspanning bij cybersecurity in vijf conceptuele raamwerken (of paradigma's) te groeperen.[36] Het betreft bescherming, rechtshandhaving, inlichtingen, conflict en een noodzakelijk en overkoepelend coördinatiemechanisme.

Verschillende departementen

Binnen de overheid zijn meerdere departementen en diensten betrokken bij cybersecurity. Bovenal het ministerie van Veiligheid & Justitie (onder meer NCTV) als coördinator met daarbinnen het Openbaar Ministerie (vervolging en opsporing strafbare feiten), de (Nationale) Politie (opsporing), het ministerie van BZK (de AIVD), het ministerie van Economische Zaken, het ministerie van Infrastructuur en Milieu, en het ministerie van Defensie (waaronder de Commandant der Strijdkrachten, de Marechaussee en de MIVD).

Defensie

Met de NCSS-1 nam de regering alvast een voorschot op het – inmiddels gestarte – strategische besluitvormingsproces binnen Defensie aangezien *'[de] responscapaciteit om ook in het digitale domein effectief te kunnen opereren wordt versterkt, onder andere bij Defensie'*.[37] Dit betreft het vierde paradigma: conflict.

Daarnaast speelt Defensie een rol bij de andere paradigma's: bescherming van het Defensie digitale domein, rechtshandhaving via de Koninklijke Marechaussee en militaire bijstand aan de politie en ten slotte inlichtingen en veiligheidsinformatie via de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en haar samenwerkingsverbanden. Defensie moest dus vier paradigma's in een beleidsvisie en strategie verwerken.

Naar een Defensie cyberstrategie

De ontwikkeling van een beleidsvisie Defensie waarin 'cyberintensiveringen' een plaats hadden, stond niet op zichzelf.[38] Het Eindrapport Verkenningen 2010 bevatte al een beleidsoverweging in die richting:

Om de inzetbaarheid van de krijgsmacht te blijven waarborgen, zal Defensie haar digitale weerbaarheid de komende jaren belangrijk moeten versterken. Uitbreiding van de digitale kennis, vaardigheden en faciliteiten is nodig. Dit impliceert het vergroten van bewustwording van dagelijkse gebruikers en de inzet van specialisten op het gebied van digitale surveillance en emergency response. Uit militair oogpunt bestaat tevens behoefte meer inzicht te krijgen in cyberoperations, zowel [als] onderdeel van offensieve operaties als bij wijze van reactie op een aanval. Nationale en

35 NCSS-1, 4.

36 Zie: Ducheine, P.A.L., Voetelink, J.E.D., Stinissen, J., Gill, T.D. (2012), 'Towards a Legal Framework for Military Cyber Operations', in: Ducheine, P.A.L., Osinga, F., Soeters, J. (eds) (TMC Asser Press, The Hague), 101-128, 110; en Ducheine, P.A.L., 2015'. 'The Notion of Cyber Operations in International Law', in: Tsagourias, N., Buchan, R. (eds) *The Research Handbook on the International Law and Cyberspace*. Cheltenham: Edwar Elgar Publishing, 211-232.

37 *Kamerstukken* II, 2010/11, 26 643, nr. 174.

38 *Kamerstukken* II 2010-11, 26 643, nr. 174.

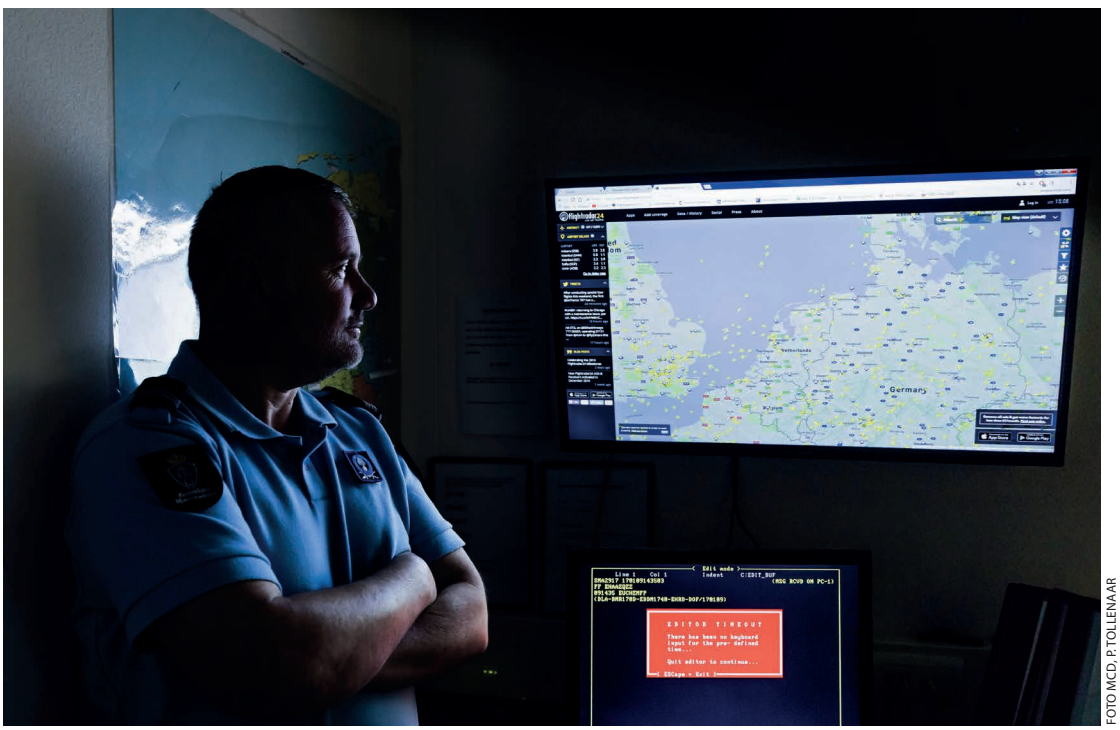


FOTO MCD, P. TOLLENAAR

Binnen de overheid zijn verschillende departementen betrokken bij cybersecurity. De Koninklijke Marechaussee (rechtshandhaving en militaire bijstand aan de politie) is er daar één van

internationale (NAVO en EU) afstemming en juridische inbedding zijn hierbij van wezenlijk belang.[39]

Ook de nota *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld,* uit 2011, meldde dat '*Defensie haar digitale weerbaarheid de komende jaren [zal] versterken en het vermogen [zal] ontwikkelen tot het uitvoeren van cyber operations*'.[40] Aan dit beleidsvoornemen was een budget gekoppeld. Incidenten in die periode zoals Stuxnet en de Diginotar affaire,[41] brachten de bekendheid van de kwetsbaarheden op een hoger peil en voedden het gevoel van urgentie.

Veronderstellingen

De parlementaire wens om cybercapaciteiten te ontwikkelen houdt niet alleen verband met de bedreigingen tegen vitale belangen, maar mogelijk ook met het niet-kinetische karakter van cyberoperations en cyberwarfare: de gedachte dan wel hoop dat langdurige en omvangrijke inzet (van grondtroepen) daarmee vermeden kan worden, alsmede de perceptie dat cyberaanvallen 'chirurgisch' schoon (lees: met weinig *collateral damage*) en minder politiek gevoelig zijn.

Of dit juiste veronderstellingen en verwachtingen zijn, valt nog te bezien. Feit is dat het advies *Digitale oorlogvoering* dat de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstuk-

39 Ministerie van Defensie, *Eindrapport verkenningen - Houvast voor de krijgsmacht van de toekomst* (2010).

40 Zie de nota *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld*, 8-4-2011, 22 van 42.

41 Diginotar was een certificeringsinstantie die gecompromitteerd bleek, waardoor Windows de door deze instantie verstrekte certificaten dreigde te blokkeren. Dit zou reguliere communicatie met bijvoorbeeld Word-documenten onmogelijk hebben gemaakt. Zie *Kamerstukken* II 2010–11, 26 643, nr. 188, met bijlage: Fox-IT, Interim report DigiNotar audit, 5 september 2011, <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf>;

ken (AIV & CAVV) in december 2011 uitbrachten,[42] na een schriftelijke ronde in juni 2012,[43] pas in het voorjaar van 2014 werd besproken.[44]

Knelpunten

Een van de grootste knelpunten voor de defensievisie behelsde het ontbreken van een integrale strategische visie: Nederland kent geen (lange) traditie met veiligheidsstrategieën. De Britse denktank Chatham House benadrukte in de studie *On Cyber Warfare* vooral de noodzaak voor een strategisch raamwerk voor cybersecurity en cyberwarfare.[45] De enige strategische documenten die naast de beleidsnota's van Defensie zelf ter beschikking waren, betroffen de Nationale Veiligheidsstrategie (2007) en de NCSS-1.[46] De Nederlandse Internationale Veiligheidsstrategie zag pas in 2013 het levenslicht.[47]

Het advies *Digitale Oorlogvoering* behandelde echter wel cruciale kwesties van politiek-strategische, militair-strategische en internationaalrechtelijke aard.[48] Daarmee beschikten de regering, Defensie en Buitenlandse Zaken in ieder geval over enige strategische fundering. De AIV & CAVV beschreven het digitale domein als: 'het geheel van ICT-middelen en ICT–diensten, [inclusief] alle niet met internet verbonden netwerken of andere digitale apparaten'.[49]

Dit digitale domein is door de mens gemaakt en bestaat uit alle 'entiteiten die digitaal verbonden (kunnen) zijn'.[50] Krijgsmachten hanteren een gelaagd model om werking en toepassing te beschrijven.[51] Het betreft een sociale laag met mensen en hun cyberidentiteiten (e-mailadressen, accounts, et cetera), een logische laag met cyberobjecten (software, applicaties, data) en een fysieke laag met hardware en geografische locaties.[52] Communicatie en informatie tussen de verschillende entiteiten in de lagen staan centraal.[53] De verschillende lagen bieden aanknopingspunten voor beïnvloeding, manipulatie en verstoring waartegen bescherming geboden is. De lagen bieden ook kansen voor het verzamelen en verwerken van informatie, alsmede voor het militair gebruik in operaties.[54]

De tevens door de AIV & CAVV aangedragen operationele drieslag, defensief-inlichtingen-offensief,[55] keerde ook als centraal element terug in de *Defensie Cyber Strategie* die minister Hillen in juni 2012 presenteerde.[56] Die drieslag sluit aan bij drie van de vier voor Defensie relevante paradigma's.[57]

Defensie cyberstrategie

Het doel van de DCS is cyberspace optimaal gebruiken om 'inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te vergroten'.[58] Het startpunt in de DCS is dat 'de drie hoofdtaken van Defensie [..] ook in het digitale domein leidend [zijn] voor de inspan-

42 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>.

43 *Kamerstukken* II 2011–12, 33 000 X, nr. 99 (Vragen en antwoorden VCD).

44 *Kamerstukken* II 2013–14, 33 321, nr. 4 (AO Defensie Cyber Strategie), 26 maart 2014. Dit stond los van de parallelle parlementaire sessies inzake het bredere cyber security die in de Vaste Kamercommissie voor V&J plaatsvonden.

45 P. Cornish, D. Livingstone, D. Clemente & C. Yorke, *On Cyber Warfare*, Chatham House, 2010, 21-22.

46 Zie Tettero & de Graaf.

47 *Kamerstukken* II *2012-13*, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland.

48 AIV & CAVV, 5: '1. Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld en kunnen worden ingezet? 2. Wat is de aard en rol van operationele cybercapaciteiten bij militaire operaties? […] 4. Onder welke omstandigheden kan een cyberaanval worden beschouwd als een gewapende aanval waartegen geweld mag worden gebruikt ter zelfverdediging op basis van artikel 51 van het VN Handvest? 5. Wanneer is er sprake van toepasselijkheid van het humanitair oorlogsrecht op gedragingen in het digitale domein?'

49 AIV & CAVV, 7.

50 C.W.M Dessens (2014) *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, in: *Kamerstukken II* 2013–14, 33 820, nr. 1 bijlage, 85.

51 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, 8. Idem: Wouter Stol (2010), *Cybersafety overwogen - Een introductie in twee lezingen*, Den Haag: Boom Juridische uitgevers.

52 P.A.L. Ducheine & J. van Haaster (2014) 'Fighting Power, Targeting and Cyber Operations', in: Brangetto, P., Maybaum, M., Stinissen, J. (eds) *Proceedings of the 6th International Conference on Cyber Conflict* (2014). CCDCOE, Tallinn, 303-328, 309.

53 Zie de minister van Defensie, in*: Kamerstukken* II 2013–14, 33 321, nr. 3, 2.

54 P.A.L. Ducheine & Jelle van Haaster (2013) 'Cyber-operaties en militair vermogen', *Militaire Spectator* 182 (9) 368-387.

55 Ook reeds in: *Kamerstukken* II 2010-11, 32 733, nr. 1, 19, Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld (8-4-2011).

56 *Kamerstukken* II 2011-12, 33 321, nr. 1 (27-6-2012).

57 De AIV&CAVV waren niet specifiek naar nationale rechtshandhaving gevraagd.

ningen van de krijgsmacht. Zij moet derhalve handelend kunnen optreden tegen een digitale bedreiging van de samenleving of van de internationale rechtsorde'.[59]
Dit sluit aan bij de eerder genoemde vitale belangen (zie figuur 1), bij de grondwettelijke doelomschrijving[60] en bij de hoofdtaken van de krijgsmacht: 'De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil ook in het digitale domein haar rol als 'zwaardmacht' naar behoren vervullen'.[61]

Om dit doel te realiseren, zijn zes 'speerpunten' gedefinieerd, waaronder drie randvoorwaardelijke:
- een integrale aanpak;
- versterking van de kennispositie en het innovatieve vermogen van Defensie in het digitale domein, inclusief werving en het behoud van gekwalificeerd personeel ('adaptief en innovatief');
- intensivering van de samenwerking in nationaal en internationaal verband ('samenwerking').

De kern van de strategie betreft de drieslag:
- versterking van de digitale weerbaarheid van Defensie ('defensief');
- versterking van de inlichtingenpositie in het digitale domein ('inlichtingen');
- ontwikkeling van het militaire vermogen om cyberoperations uit te voeren ('offensief').

De integrale aanpak had al geresulteerd in de instelling van de Task Force Cyber, die de coördinatie over en de uitwerking van de speerpunten ter hand moest nemen. De DCS omvat duidelijk herkenbaar drie paradigma's: bescherming, inlichtingen en conflict. Het rechtshandhavingsparadigma (voor de Koninklijke Marechaussee) ontbreekt vooralsnog, hoewel dit bij een enkeling wel in beeld is.[62]
De – in totaal – vier cyber security paradigma's waaraan defensie bijdraagt, resulteren in vier onderscheidende cyberrollen binnen defensie.[63] De rollen kennen elk hun eigen juridische en bestuurlijke raamwerk, zijn veelal ondergebracht bij verschillende defensieonderdelen, en kennen hun eigen taken, bevoegdheden en verantwoordingslijnen.

Figuur 3 Vier digitale rollen Defensie

Bescherming
De eerste rol betreft *bescherming (of beveiliging)* van de interne bedrijfsvoering in vredestijd alsmede (ondersteuning van de) commandovoering tijdens inzet.[64] De rol omvat taken voor bijvoorbeeld Joint Informatievoorzieningscommando, DefCERT, de afdeling (ICT) Operations van de Defensie Materieel Organisatie, de Beveiligingsautoriteit, maar ook voor de MIVD.

Deze rol treft ook de individuele militair, commandanten en leidinggevenden omdat dit ook de handhaving van interne veiligheidsvoorschriften omvat. Kennisverbetering, scholing, bewustwording en weerbaarheid, maar ook fysieke beveiliging, kwaliteitseisen voor systeemontwerp, hard- en software horen bij deze rol.

58 DCS, 2 en *Kamerstukken* II 2014-15, 33 321, nr. 5, Actualisering Defensie Cyber Strategie, 1.
59 *Kamerstukken* II 2011-12, 33 321, nr. 1, Defensie Cyber Strategie, 2. (hierna DCS).
60 Zie art. 97 Grondwet en P.A.L. Ducheine & K.L. Arnold (2015), 'Besluitvorming bij cyberoperaties', *Militaire Spectator* 184 (2015) (2) 56-70.
61 DCS, 2.
62 Editoriaal 'Marechaussee & cyber', in: *Militaire Spectator* 182 (2013) (6) 278-279.
63 Ducheine (2015 in Tsagourias).
64 Ducheine (2015 in Tsagourias), 221. Zo ook A. Klimburg & P. Mirtl, 'Cyberspace and Governance—A Primer'Austrian Institute for International Affairs . Zie: <http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf> (benaderd 11 November 2013); en A. Klimburg (ed.) *National Cyber Security Framework Manual* (CCD COE 2012).

Rechtshandhaving
De tweede rol betreft *rechtshandhaving*. De Koninklijke Marechaussee, een militaire politieorganisatie die beheersmatig bij Defensie is ondergebracht maar qua rechtshandhaving onder civiel gezag opereert, speelt voor defensie zelf een rol (op objecten in beheer bij defensie; jegens de strijdkrachten), maar ook op andere terreinen waar zij op grond van art. 4 Politiewet 2012 bevoegd is.

Daarnaast kan de krijgsmacht (inclusief Koninklijke Marechaussee) bijstand leveren aan de civiele politie op grond van art. 57-58 Politiewet 2012. Zij treedt dan op onder civiel gezag (burgemeester c.q. officier van justitie dan wel de minister van Veiligheid en Justitie).

Inlichtingen
Ten derde is er de *inlichtingenrol*. Dit ligt uiteraard bij de MIVD, die naast interne intensivering samen met de AIVD een *Joint Sigint Cyber Unit* (JSCU) oprichtte.[65] Deze eenheid heeft als taken: het verwerven van gegevens uit technische bronnen; het ontsluiten van gegevens uit technische bronnen; ondersteuning bij analyse; het leveren van Signals intelligence en cybercapaciteit. De reguliere taken van de MIVD die verband houden met het digitale domein liggen besloten in de Wet op de inlichtingen- en veiligheidsdiensten 2002.[66]

Conflict
De vierde rol ligt in het domein van de Commandant der Strijdkrachten (en de operationele commando's): de inzet van operationele cybercapaciteiten die *conflict*-gerelateerd zijn.

Een operationele cybercapaciteit omvat alle kennis en middelen die nodig zijn om gedurende operationele inzet langs digitale weg het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken, en zich te verdedigen tegen vergelijkbaar handelen door de tegenstander. Dit gebeurt door infiltratie van computers, computernetwerken, wapen- en sensorsystemen en software om informatie en inlichtingen te vergaren en systemen te beïnvloeden. Een operationele cybercapaciteit omvat dus inzetbare defensieve, inlichtingen- en offensieve elementen.[67]

Deze rol is toebedeeld aan het nieuwe Defensie Cyber Commando (DCC), dat – na reorganisatieperikelen – daadwerkelijk in juni 2015 is opgericht.[68] Het DCC, een krijgsmachtbrede ('joint') eenheid, is administratief ondergebracht bij het Commando Landstrijdkrachten. Het omvat een Defensie Cyber Expertise Centrum (DCEC), een technische poot en een operationele poot. De technische poot ontwikkelt cybercapaciteiten en deelt kennis met specialisten uit de andere drie rollen. De operationele poot vormt de verbinding tussen technische expertise en de eindgebruikers: militaire commandanten.

In de DCS is het DCEC aangewezen als centrale kennisorganisatie voor Defensie en is het verantwoordelijk voor kennisontwikkeling, borging en verspreiding binnen de gehele defensieorganisatie. Het DCEC heeft relaties met externe en interne kennisinstituten, en organisaties als TNO, *NATO's Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn en de leerstoel Cyber Operations & Cyber Security van de Nederlandse Defensie Academie. Deze leerstoel en het DCEC geven beide mede invulling aan de speerpunten kennis, innovatie en samenwerking.

De operationele cybercapaciteit varieert van defensief tot offensief, van inlichtingen verzamelen binnen de verantwoordelijkheid van de Commandant der Strijdkrachten (CDS) tot het beïnvloeden van actoren via het digitale domein. Dit kan uiteindelijk uitmonden in disruptieve acties tegen opponenten.[69]

65 *Kamerstukken* II 2013-14, 29 924, nr. 113 (Oprichting en convenant JSCU).
66 Zie de taken in art. 7 Wiv 2002 en de daarbij te hanteren bevoegdheden in artt. 12, 17, 20-30. Voor een evaluatie van de wet, zie Dessens (2014).
67 DCS, 4-5.
68 Aanvankelijk zou het DCC in 2015 worden opgericht. In de nota 'In het belang van Nederland' (Kamerstukken II, 2013-14, 33 763, nr. 1) werd dit versneld beoogd in 2014. Minister Hennis-Plasschaert gaf op 25 september 2014 dan ook het 'virtuele' startschot, maar reorganisatieperikelen vertraagden dit. Zie: <http://www.defensie.nl/actueel/nieuws/2014/09/25/minister-geeft-startschot-voor-defensie-cyber-commando>.
69 Voor een overzicht van de diverse opties: Ducheine & van Haaster (2013). Disruptief heeft hier een brede betekenis (Van Dale: verbrekend, verwoestend) en omvat ook '*destroy, degrade, disrupt, deny*'.

Weinig aandacht voor constructieve capaciteiten

Tot nu toe heeft constructieve toepassing in Nederland weinig aandacht gekregen. Het betreft bijvoorbeeld *information operations* die een positief beeld wegzetten van de eigen inzet via *social media*. Bijvoorbeeld via het plaatsen van beeldmateriaal van een F-16 of Apache dat de zorgvuldige besluitvorming van vliegers bij luchtaanvallen demonstreert.

Buitenlandse initiatieven, zoals de oprichting van 77 (UK) Brigade die de 'focal point for levers of soft power […] or persistent engagement' is, brengen hier mogelijk verandering in. De aandacht voor informatieoperaties waarbij het digitale domein als medium fungeert, waarbij beelden en beeldvorming centraal staat, groeit gestaag. Het is niet vreemd in Nederland als de CDS zijn 'soft' power capaciteiten, anders dan nu, zou (laten) organiseren.[70]

De meeste aandacht van onder andere media en parlement gaat uit naar disruptieve, offensieve capaciteiten. Deze beogen met cyberoperaties schade of verstoring/vertraging te veroorzaken bij anderen (onder wie tegenstanders). Dit betreft cyberwarfare in de definitie van het AIV:

het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen.[71]

Het gaat – in de context van militaire operaties die aan de CDS zijn toevertrouwd – bijvoorbeeld om de inzet van *malware* (zoals bijvoorbeeld Stuxnet), afvangen en manipuleren van communicatie, digitale *social engineering*, et cetera. Minister Hennis wijdde een aparte brief aan deze capaciteit:

Offensieve cybercapaciteiten zijn de digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten.[72]

FOTO MCD, A. SALAMPESSY

Minister Hennis van Defensie wijdde een aparte brief aan de inzet van offensieve cybercapaciteiten

Ten tijde van het uitbrengen van de DCS stelde de regering:

De ontwikkeling van offensieve operationele capaciteiten staat internationaal nog in de kinderschoenen. Er is nog veel onduidelijk over de aard van deze capaciteiten, de mogelijkheden die ze kunnen bieden en de effecten die ermee kunnen worden gesorteerd.[73]

Alsof zij die onduidelijkheid wilde benadrukken, hanteert de regering zelf een eenzijdig beeld van deze offensieve capaciteiten door te stellen dat deze zich *van conventionele militaire capaciteiten [onderscheiden] doordat ze vaak slechts eenmalig inzetbaar zijn en veelal een beperkte levensduur hebben.*[74]

Deze focus op eenmalige, in tijd kritisch inzetbare cybercapaciteiten valt samen met een nadruk op hoogtechnologische capaciteiten, zo blijkt:

Hoogwaardige cybercapaciteiten zijn nauwelijks vergelijkbaar met algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden. Het gaat hier om complexe middelen waarvan de ontwikkeling zeer kennisintensief is en daardoor

70 Zie: <https://britisharmedforcesreview.wordpress.com/2015/01/31/the-security-assistance-group-now-the-77th-brigade/>.
71 AIV & CAVV (2011), 8.
72 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.
73 DCS 2012, 7 (Kamerstukken versie).
74 DCS 2012, 7 (Kamerstukken versie).

kostbaar en tijdrovend. Een uitdaging is dat de gewenste effecten moeilijk gegarandeerd kunnen worden doordat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken.[75]

Hoe het ook zij, het fameuze Stuxnet is meermaals en gedurende langere tijd ingezet in Iraanse nucleaire faciliteiten.[76] Ook 'algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden'[77] zoals DDoS-aanvallen kunnen vaker gebruikt worden tijdens conflictsituaties.[78] En sommige ICT-systemen worden ondanks bekende cyberbedreigen bewust slechts mondjesmaat van softwareaanpassingen voorzien.[79] Daarnaast waant men zich regelmatig veilig vanwege een (van internet) losstaand *Industrial Control System* van internet, en blijft repareren van kwetsbaarheden, *patchen,* (daardoor) soms achterwege.[80] Bovendien zou bijna vergeten worden dat naast deze op cyberobjecten gerichte aanvallen, het ambachtelijke kraken van toegangscodes, het via *social engineering* toegang verkrijgen tot cyberidentiteiten (onder meer administrator accounts), een andere aanvalsmethode is. Ook op deze cybercapaciteit past de hoogtechnologische, vergankelijke en tijd-kritische typering niet.[81]

Recente Kamerbrieven

Recentere Kamerbrieven bevatten gelukkig een nuancering:

Dit laat onverlet dat in operaties ook kan worden gebruikgemaakt van minder complexe en mogelijk laagdrempelige cybercapaciteiten. Maar ook hiervoor is een goede inlichtingenpositie onontbeerlijk.[82]

De actualisering van de DCS van februari 2015, zet deze draai verder kracht bij:

Offensieve cybermiddelen kunnen variëren van relatief eenvoudig en snel te ontwikkelen middelen met een tactische impact tot aan middelen met een hoge, strategische impact die een lange ontwikkelingstijd vergen.[83]

De actualisering uit 2015 benadrukt daarnaast dat cybercapaciteiten in een breed spectrum van gewenste effecten kunnen worden ingezet: van strategisch tot tactisch. Gecombineerd met een technische variëteit van laagwaardig tot hoogwaardig zijn zo verschillende capaciteiten te duiden: hoogtechnologisch/strategisch, hoogtechnologisch/tactisch, laag-technologisch/strategisch en laag-technologisch/tactisch.

Deze vierdeling kan verder gedifferentieerd worden naar de aard van de gewenste effecten, oftewel het doel van de inzet, en kan variëren van (tijdelijk of permanent) disruptief (inclusief vernieling) tot constructief.[84] Dat laatste gebruik sluit aan bij de eerder genoemde notie van soft power, van beïnvloeding via het informatiedomein, in dit geval cyberspace.[85]

Deze uitbreiding van mogelijkheden sluit aan bij de notie dat de krijgsmacht effecten en beïnvloeding van actoren in militaire operaties centraal stelt.[86] Deze *effect-based* en *manoeuvrist approach* onderstreept dat de doelstelling van

75 DCS 2012, 7 (Kamerstukken versie). Idem: *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.

76 Ralph Langner, *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (November 2013), via < www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>; Sanger, David (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown. Het moment van lokale ontdekking en publieke bekendheid kunnen verschillen.

77 DCS 2012, 7 (Kamerstukken versie).

78 Waarbij een slachtoffer zich uiteraard kan beschermen. Zie o.a. Carol Matlack, 'Cyberwar in Ukraine Falls Far Short of Russia's Full Powers,' *Bloomberg Business Week*, <businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers> (accessed March 11, 2014).; See also: Reuters, 'Ukrainian Authorities Suffer New Cyber Attacks,'Reuters, <reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308> (accessed March 11, 2014).; Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (New York: Syngress, 2014), 139

79 Zoals o.a. bij labiele *legacy* systemen waarbij *patchen* onvermoede complicaties veroorzaakt.

80 Ook losstaande (*air-gapped*) systemen kunnen bijvoorbeeld met akoestische signalen benaderd worden. Zie: Michael Hanspach & Michael Goetz (2013) 'On Covert Acoustical Mesh Networks in Air', in: *Journal of Communications* 8 (11), 758-767.

81 Voor een overzicht van methoden en technieken: Ducheine & Haaster (2014), 317-328.

82 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.

83 *Kamerstukken* II 2014-15, 33 321, nr. 5, 11.

84 Zie hiervoor Ducheine & van Haaster (2013), 386.

85 Zie het gebruik van social media door ISIS: J.M. Berger & Jonathon Morgan (2015). *The ISIS Twitter Census - Defining and describing the po pulation of ISIS supporters on Twitter* Brookings Institute; Christina Schori Liang (2015) *Cyber Jihad: Understanding and Countering Islamic State Propaganda* GCSP Policy Paper 2015/2.

86 Zie Ministerie van Defensie, *Netherlands Defence Doctrine*, 2013. <http://www.defensie.nl/binaries/defensie/documenten/publicaties/2013/11/20/defence-doctrine-en/defensie-doctrine_en.pdf> banderd 16 maart 2014 (p. 111). The Hague; en Koninklijke Landmacht. (2015). Doctrine Publicatie 3.2 Landoperaties (DPLO 3.2).

FOTO MCD, E. KLIJN

Sinds begin 2014 doet de Islamitische Staat in Irak en Syrië meermaals en vaak barbaars van zich spreken. In de coalitie tegen ISIS leek aanvankelijk geen plaats voor Nederland te zijn voorzien

militaire operaties (cyberoperaties incluis) niet alleen het verslaan van opponenten is. Ook andere (zijdelings) betrokken partijen, zoals de bevolking in een missiegebied, bondgenoten, neutrale partijen, afzijdige partijen, kunnen beïnvloed worden.

De actualisering van de DCS

De in het Algemeen Overleg van 26 maart 2014 (waarin het AIV-CAVV-advies 'Digitale oorlogvoering' en de DCS werden besproken) toegezegde actualisering van de DCS is op 23 februari 2015 aan het parlement aangeboden.

De actualisering werd beïnvloed door een aantal – voor Defensie relevante – gebeurtenissen. In chronologische volgorde betreft dit allereerst de onthullingen van Edward Snowden vanaf juni 2013.[87] Kort daarop verscheen de *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, van de Commissie Dessens.[88] De eerder genoemde brief over 'offensieve cybercapaciteiten' van 17 maart 2014 dateerde nog van voor het algemeen overleg.[89]

Op het wereldtoneel culmineert de crisis om de Krim ondertussen in de annexatie van de Krim door Rusland op 18 maart 2014. De vlam slaat sindsdien in de pan in (Oost-) Oekraïne. En sinds het voorjaar van 2014 doet de Islamitische Staat in Irak en Syrië (ISIS of Daesh) meermaals en vaak barbaars van zich spreken.

In juni 2014 bracht het NCSC inmiddels het vierde Cyber Security Beeld Nederland uit. In

87 Zie o.a. Luke Harding (2014) *The Snowden Files: The Inside Story of the World's Most Wanted Man (Pb ed.): Vintage.*

88 C.W.M Dessens (2014) *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, in: *Kamerstukken II* 2013–14, 33 820, nr. 1 bijlage.

89 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten.

november 2014 reageerde de regering op de evaluatie van de Commissie Dessens inzake de modernisering van de Wet- op de inlichtingen en veiligheidsdiensten.[90] En na de NAVO-top in Wales is Nederland figuurlijk 'te klein' omdat in de coalitie tegen ISIS aanvankelijk geen plaats voor Nederland lijkt te zijn voorzien. Begin januari schrikt Europa van aanslagen in Parijs, onder andere op de redactie van het tijdschrift Charlie Hebdo, en van een ingreep van justitie en politie in Verviers, België.

Speerpunten

Tegen deze achtergrond, herhaalt de minister van Defensie eerst dat de 'digitale revolutie' kansen biedt om de 'doeltreffendheid en de doelmatigheid van het militaire optreden wezenlijk te bevorderen'.[91] Zij houdt in grote lijnen vast aan de DCS uit 2012, waarbij zij – naast de trits weerbaarheid, inlichtingenvermogen, operationele capaciteit – vier randvoorwaardelijke speerpunten noemt. Het gaat om boeien, binden en ontwikkelen van cyberprofessionals; innoveren; bundelen en samenwerken; en kennis verdiepen.

Vooral op het DCC, de operationele cybercapaciteit, geeft de Kamerbrief verdieping ten opzichte van de DCS:

Om de verantwoorde en doeltreffende inzet van digitale middelen in militaire operaties mogelijk te maken, zal Defensie de komende tijd in het bijzonder aandacht geven aan:

- *de verdere ontwikkeling van een Defensie Cyber Doctrine;*
- *de ontwikkeling van offensieve cybermiddelen en van richtlijnen voor de gereedstelling van flexibel samen te stellen cybereenheden en cybermiddelen;*
- *de inrichting van defensieve digitale middelen bij missies;*
- *de ontwikkeling van cyber(inlichtingen)middelen voor tactische inzet;*
- *de integratie van cyberaspecten in het operationeel besluitvormingsproces, voorafgaand aan en tijdens operaties.*[92]

Onder het speerpunt 'samenwerking' komt na lang touwtrekken uiteindelijk ook de Koninklijke Marechaussee in beeld. Als politieorganisatie werd zij niet expliciet in de NCSS-1 en -2 genoemd. Maar gelet op de algemene en de specifieke taken was al duidelijk dat zij 'geraakt' zou worden door de toename van digitale ontwikkelingen.

Ook het voorziene wetsvoorstel Computercriminaliteit III raakt de Marechaussee door de voorgestelde introductie van nieuwe strafbaarstellingen en opsporingsbevoegdheden. Bovendien leidt inzet van het Defensie Cyber Commando tot een extra rol in de *ex post* beoordeling van militaire operaties, zoals dat bij fysieke operaties (regulier of speciaal) al het geval is.

Nuancering van cybercapaciteiten

Een ander markant punt in de actualisering is de nuancering van cybercapaciteiten. Waar deze voorheen vrij eenzijdig als strategisch, hoogtechnologisch, vluchtig en tijd-kritisch werden aangemerkt, herkent de minister nu ook tactische, eenvoudigere, meermalig en niet-tijdgebonden inzetbare capaciteiten. Of zij daarmee ook (al) oog heeft voor 'soft' cybercapaciteiten voor constructieve effecten of dat het digitale domein slechts dient als medium voor het overbrengen van effecten, bijvoorbeeld ter beïnvloeding, is zeer de vraag.

De Oekraïne-crisis en de strijd tegen ISIS bevestigen dat niet slechts fysieke actie maar vooral informatie en communicatie als boodschap en 'wapen' wordt aangewend.[93]

Cybersecurity: vitaal belang?

Niet-statelijke actoren, zoals ISIS, terroristische en criminele netwerken, maar ook multinationals, internationale organisaties, gelegenheidscoalities van burgers (bijvoorbeeld tijdens de Arabische Lente) of belangengroepen (bijvoor-

90 *Kamerstukken* II 2014–15, 33 820, nr. 4.

91 *Kamerstukken* II 2014-15, 33 321, nr. 5, 1.

92 *Kamerstukken* II 2014-15, 33 321, nr. 5, 11.

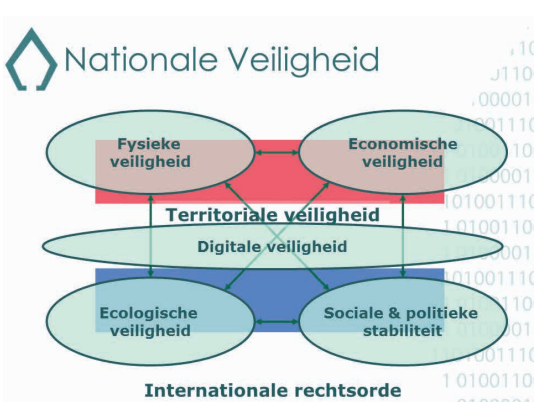
93 Zie ISIS' *Al-Hayat Media Centre* <http://jihadology.net/category/al-%E1%B8%A5ayat-media-center/> en het tijdschrift *Dabiq*, <www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq>, evenals Al Qaida's *Al-Shahab*, in: Carloen Roelants 'Terrorisme bestaat niet zonder communicatie - De mediastrategie van IS', *NRC Handelsblad* (16-9-2014).

FOTO ANP, F. VAN DEN BERGH

Ook niet-statelijke actoren, waaronder gelegenheidscoalities van burgers of belangengroepen zoals GeenPeil, manifesteren zich steeds vaker als machtsspeler

beeld GeenPeil 2.0) manifesteren zich – in toenemende mate – ook als machtsspeler. Informatie als machtsbron is in het huidige digitale tijdperk toe aan een herwaardering.[94]

Via directe dwang (dreigen met onthulling), door institutionele (sleutelposities binnen ICANN)[95] of structurele macht (Microsoft, met het besturingssysteem Windows) is dit bekend terrein. Maar vooral als productieve machtsfactor komt informatie toenemend tot wasdom.



Figuur 4 Nationale veiligheid met zeven vitale belangen

Dat wil zeggen dat actoren met informatie agenda's kunnen vormen en een debat kunnen starten, versterken en beïnvloeden.[96] Dit geheel faciliteert nieuwe 'elites' en actoren.

De proliferatie van ICT en de brede maatschappelijke afhankelijkheid van ICT brengt onze (interdependente) vitale economische, bestuurlijke, politieke en sociale processen binnen het bereik van deze actoren. Een geavanceerde digitale samenleving en economie is dus niet slechts een zegen én een machtsfactor, maar ook een kwetsbare en alle vitale belangen doorsnijdende factor.[97] In dat opzicht zou ons begrip van nationale veiligheid ondertussen best een zevende vitale belang kunnen bevatten: digitale veiligheid (zie figuur 4).[98]

94 Zie o.a. Jelle van Haaster, Assessing Cyber Power, in: N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), *8th International Conference on Cyber Conflict: Cyber Power*, Tallinn: CCDCOE, 2016, via: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20Assessing%20Cyber%20Power.pdf>

95 ICANN verzorgt onder meer domeinnamen en IP-nummers.

96 David Betz & Tim Stevens, Power and cyberspace, *Adelphi Series*, 2011.

97 McKinsey Global Institute, *Digital globalization: The new era of global flows*, March 2016, via: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

FOTO MCD, G.VAN ES

Cybersymposium op de NLDA: een geavanceerde digitale samenleving is ook kwetsbaar

Tot slot

Inmiddels liggen twee genoemde wetsvoorstellen, *Wet Computercriminaliteit III* en *Wet op de inlichtingen en veiligheidsdiensten 20..* [sic], in de Eerste Kamer. Het parlement is dus aan zet.[99] Die voorstellen en de parlementaire reactie zijn bepalend voor de uiteindelijke bevoegdheden en taakvervulling van respectievelijk de Marechaussee en de MIVD. Met het feit dat het DCC in de loop van 2017 operationeel wordt en de voortdurende inspanningen om de defensie-ICT beveiliging te verbeteren, zijn er voldoende impulsen voor verdere ontwikkelingen.

Het idee dat informatie, communicatie en de informatieomgeving, waarvan cyberspace deel uitmaakt, de volgende *high grounds* voor toekomstige inzet worden, heeft inmiddels stevig postgevat.[100] Dit uit zich in een toename aan beschouwingen, analyses en studies naar (para)militaire activiteiten in het digitale domein.[101] De aandacht voor hybride dreigingen helpt daarbij. De notie dat complexe veiligheidsproblemen niet zonder multidisciplinaire benadering zijn aan te pakken, krijgt gelukkig steeds meer steun.[102]

Hoe dit uitpakt voor het monopolie van het DCC, cyberwarfare, laat zich raden nu de Verenigde Staten en het Verenigd Koninkrijk hun eerste digitale wapenfeiten in de strijd tegen ISIS publiekelijk hebben gemaakt. Het feit dat ook de NAVO (eindelijk) de notie van cyberspace als een operationeel domein onderzoekt, spreekt overigens boekdelen. Cyberwarfare is realiteit geworden.[103] ■

98 In die zin moet ook het pleidooi voor een minister-zonder-portefeuille voor ICT worden verstaan, in: *Het Financieele Dagblad*, 'Kabinet heeft minister van ICT nodig' (10 januari 2016), via: <https://fd.nl/economie-politiek/1134298/kabinet-heeft-minister-van-ict-nodig>. Hoewel de petitie daarvoor heden (21-9-2016) slechts 316 ondertekeningen kent, zie: < http://ministervanict.nl/>.

99 Zie P. A.L. Ducheine, 'Mythen over digitale oorlogvoering en recht', *Militaire Spectator* 185 (2016) (3) 131.

100 Zie bijvoorbeeld de oprichting van de 77 (UK) Brigade, <https://britisharmedforces-review.wordpress.com/2015/01/31/the-security-assistance-group-now-the-77th-brigade/> en A. Schnitger, 'De luchtmacht in het security ecosysteem', *Militaire Spectator* 185 (2016) (7/8) 301.

101 Zie onder meer de publicaties van NATO's STRATCOM Centre of Excellence, <http://www.stratcomcoe.org/publications>.

102 Zie onder meer de afzonderlijke bijdragen van Frans Osinga, Rob de Wijk en Paul Ducheine in het themanummer van het Magazine Nationale Veiligheid <https://www.nctv.nl/onderwerpen_a_z/mnvc/index.aspx>.

103 Zie P. A.L. Ducheine, 'Cyber warfare is taking place', *Internationale Spectator* 70 (2016) (6) <https://www.internationalespectator.nl/pub/2016/6/>.

De Baltische staten, de Russische minderheid en de verdediging van de NAVO

Eind 2016 reisde klas Hogere Defensie Vorming (HDV) 13.1 door de Baltische staten om zich een beeld te vormen van de mogelijke dreiging door Rusland en het antwoord dat de NAVO hierop geeft. Een conclusie is dat de dreiging bestaat, maar dat zij moet worden genuanceerd. Er bestaat een gevoel van onveiligheid, vooral in Letland en in mindere mate in Estland en Litouwen. Dit onveilige gevoel is na de verkiezing van Donald Trump tot president van de VS verder toegenomen. Ook werd duidelijk dat van 'de' Baltische staten of 'de' Russische minderheid veel minder sprake is dan men vaak veronderstelt. Door dit laatste is er voor Rusland minder aanleiding voor het starten van een oorlog dan in Oekraïne het geval was. Desondanks gaat Rusland gestaag door met het plaatsen van militaire capaciteiten rond de Baltische staten. Is het denkbaar dat Rusland de Baltische staten wil inlijven?

*Dr. J.E. Noll e.a.**

De Baltische staten zijn de achilleshiel van de NAVO. Althans, zo formuleert Agnia Grigas het in haar boek *Beyond Crimea: The New Russian Empire*. Anders dan de overige staten van het voormalig Warschaupact en de Sovjet-Unie beschouwen veel Russen (en Moskou) deze staten volgens haar nog steeds als een onderdeel van het grote Russische rijk. Belangrijke redenen hiervoor zijn Ruslands historische banden met deze landen en een grote Russische minderheid in vooral Estland en Letland.[1]

Dit laatste zou volgens Grigas een belangrijke reden kunnen zijn waarom Rusland op korte tot middellange termijn de Baltische staten binnenvalt en bezet. In dit artikel willen we laten zien dat het inderdaad denkbaar is dat de Russische president Poetin en de zijnen de Baltische staten willen inlijven. Anderzijds leent de Russische minderheid zich, anders dan misschien op de Krim, niet per se als reden voor oorlog, laat staan dat deze met grote aantallen een invasie gaat ondersteunen. Sowieso behoeft de uitspraak 'de Russische minderheid' enige nuancering, net als ons beeld van 'de Baltische staten', die deze aanduiding overigens ontlenen aan de prachtige barnsteen, die in grote hoeveelheden in de regio wordt gevonden.

* Klas 13.1 van de Hogere Defensie Vorming bestaat uit de volgende deelnemers: mr. I.C. Veltens, R.E.W. Pieters, drs. B.B. Pieters, G.C. Lieftink, ing. J.T.A. van Leeuwen, J.R. ter Veer MSc, M. Cohrs, mr J. Clayden, W.L. van Leussen, G.W. van Beek, drs. C.M.A. Vermuë en H.J. Dubbelhuis BSc. Allen hebben aan het totstandkomen van dit artikel bijgedragen. Dr. J.E. Noll, OTL d.R. is universitair hoofddocent Conflictstudies aan de Faculteit Militaire Wetenschappen.

1 A. Grigas, *Beyond Crimea: The New Russian Empire* (Yale, Yale University Press, 2016) 136.

FOTO ANP

Intocht van het Rode Leger in Kaunas, Litouwen, augustus 1944. De Baltische staten waren een speelbal tussen de Duitse bezetter en het oprukkende Rode Leger

Centraal in dit artikel staat de vraag of de Baltische staten en hun Russische minderheden voor de NAVO een veiligheidsprobleem zijn en zo ja, waarom. We gaan daartoe eerst kort in op de historische en politieke verschillen tussen Estland, Letland en Litouwen. Daarna zwakken we het westerse beeld van 'de Russische minderheid' in deze landen af. Vervolgens gaan we in op de plannen en het optreden van de NAVO in deze landen en de inspanningen van de landen zelf. We sluiten af met een overzicht van mogelijke uitdagingen en verwachtingen. We baseren dit artikel en ons oordeel op gesprekken met meer dan dertig experts, politici, ambtenaren, militairen en diplomaten in deze landen, aangevuld met mediaberichtgeving en andere (historische) wetenschappelijke analyses.

Een beladen verleden

Wie binnen enkele dagen door alle drie de landen reist en met name de hoofdsteden bezoekt, valt meteen op dat ze naast enkele overeenkomsten, grote verschillen vertonen. Tallinn, de hoofdstad van Estland, is een oude Hanzestad, met zelfs nog enkele gebouwen uit deze tijd. Daarnaast duiden tal van verschillende bouwstijlen op Duitse, Russische en Scandinavische invloeden. In het Letse Riga

daarentegen, zijn de meeste sporen van de Russische bezetting te zien, terwijl Vilnius, de hoofdstad van Litouwen, wat meer kosmopolitisch aandoet. Vilnius heeft een weidse en moderne stadsinrichting, met prachtige barokke en tsaristische gebouwen en musea.

Speelbal

Zo verschillend deze steden zijn, zo anders is ook de geschiedenis van de landen die als 'Baltische staten' bekend staan. Dit begrip is overigens pas na de Eerste Wereldoorlog ontstaan, nadat de landen hun onafhankelijkheid zwaar hadden bevochten.[2] Ook toen al waren de landen een speelbal tussen de (terugtrekkende) Duitse bezetter en het oprukkende Rode Leger. Dit herhaalde zich tijdens de Tweede Wereldoorlog, waarbij het Molotov-Ribbentrop pact een bijzondere dynamiek aan de opeenvolgende bezettingen gaf.

Tot op de dag van vandaag lijkt dit pact een grote rol te spelen in de beleving van de bewoners van de drie staten. Dit komt niet in de laatste plaats vanwege de lange bezetting door de Sovjet-Unie, die op het einde van de Tweede Wereldoorlog tot aan 1991 volgde.

Met de onafhankelijkheid probeerden de landen ieder voor zich een eigen nationaliteit en identiteit te creëren.[3] Terwijl Estland met zijn Fins-Oegrische taal meer als een Scandinavisch land oogt, is Litouwen veel meer, vanwege de historische en katholieke banden, met Polen verwand. Het Pools-Litouwse rijk behoorde sinds 1795 tot aan de Eerste Wereldoorlog tot het Russische rijk. Estland en Letland daarentegen zijn door de eeuwen heen door Duitse adel, clerus en kooplieden bestuurd. Net als in de rest van Europa ontstond ook in deze landen tijdens de Romantiek een nationaal bewustzijn.[4]

Nieuwe start

Tussen de wereldoorlogen in probeerden de drie landen een nieuwe start naar onafhankelijkheid te maken, die zowel economisch als politiek mislukte. Hier is een duidelijke parallel te trekken met andere jonge democratieën tijdens het interbellum, zoals de Republiek van Weimar. Daar waar de economie, gebaseerd op industrie en/of landbouw, zich beperkt ontwikkelde, hadden de nieuwe staatsstructuren weinig kans. Na ineffectieve, radicale agrarische hervormingen in Estland, Letland en in mindere mate Litouwen, lukte het wel om de macht van de (vaak niet-etnische) herenboeren te breken. Economisch konden de hieruit voortkomende kleine boeren echter niet concurreren op de wereldmarkt. Daarnaast, zoals Tauber beschrijft, wendde de elite zich snel van de nieuwe democratische structuren af.[5] In alle drie landen kwamen uiteindelijk autoritaire leiders aan de macht.

Randy Noorman heeft in de *Militaire Spectator* al eens eerder uitgebreid stilgestaan bij de gevolgen van de historische relatie Duitsland-Rusland voor Estland.[6] Wij willen dan ook niet té uitgebreid ingaan op het verdere verloop van de bezetting door Duitsers en Russen.

Bijzonder is dat met name de gesprekspartners uit Estland en Letland de indruk gaven dat de Russische overval en de uiteindelijke bezetting zwaarder in het collectieve geheugen is gegrift dan de Duitse bezetting. Wellicht hangt dit samen met de verschillen in duur van bezetting, maar nog waarschijnlijker is het dat ook de aard van het systeem en de manier van bezetting een rol spelen. Veelal werden de Duitsers tijdens de Tweede Wereldoorlog als bevrijders van het Russische regime beschouwd, dat op zijn beurt voor de deportatie van grote delen van de elite verantwoordelijk was.

Tweedeling

Deze indruk werd in het Bezettingsmuseum in Riga bevestigd, nadat duidelijk werd dat er nog steeds een tweedeling in de Letse maatschappij

2 J. Tauber, 'Die Geschichte der baltischen Staaten bis 1945', in M. Knodt, S. Urdze (Hrsg.), (Wiesbaden, Springer VS, 2012) 17.
R. Noorman, 'Betwist verleden: Estland tussen het Oosten en het Westen', in: *Militaire Spectator* 185 (2016) (4) 165-174.

3 J. Tauber 2012, 19.

4 E. Gerberding, 'Wissenswertes über das Baltikum', in C. Baumeister, E. Geberding, J. Könnecke, C. Nowak, *Baltikum* (Ostfildern, Dumont, 2015) 10.

5 J. Tauber 2012, 19-20.

6 R. Noorman, 'Betwist verleden. Estland tussen het Oosten en het Westen', in: *Militaire Spectator* 185 (2016) (4) 165-174.

FOTO HOLLANDSE HOOGTE, B. VERHOEFF

Riga, Letland, 1991: het einde van de sovjetbezetting. Nog steeds bestaat er een tweedeling in de Letse maatschappij tussen degenen die de Russen als bevrijders zien en degenen die de hen als bezetters bestempelen

bestaat tussen degenen die de Russen als bevrijders zien en degenen die de Russen tot op de dag van vandaag als bezetters bestempelen. We mogen daarbij niet vergeten dat Letten tijdens de oorlog aan beide kanten en ook tegen elkaar vochten. In het collectieve geheugen zit ook verankerd dat de Letse president, Kärlis Ulmanis, het in juni 1940 niet aandurfde op te treden tegen de Russische inval.[7]

De herinneringen aan de Russen is in de drie landen nog zeer levendig. Dit komt door de langdurige sovjetbezetting van de Baltische landen tot aan de val van de Berlijnse muur, en daarnaast door de aanwezigheid van de Russischtalige minderheden. Naast de sociale problemen die de aanwezigheid van de minderheden met zich meebrengt, beschouwt men hen ook als een veiligheidsprobleem. Net als in Oekraïne of Zuid-Ossetië zou vooral de Russische minderheid een reden voor het Rusland van Poetin kunnen zijn om de Baltische staten binnen te vallen en te annexeren.

De Russische minderheid?

De Russische invloed op de Russischtalige minderheden in de Baltische staten wordt vaak gezien als een onderdeel van hybride oorlogvoering en soms als Russische *soft power* in de vorm van *public diplomacy*. Volgens Coombs en Holladay omvat dit '*the efforts of governments from one nation to send messages directly to the "people" in another country and is part of soft power*'.[8] Met andere woorden, '*soft power is about making others want to support you, by making it appealing for them to do so*'.[9]

7 A. Rikveilis, 'Latvia', in H. Biehl, B. Giegerich, A. Jonas (Eds.) *Strategic Cultures in Europe: Security and Defence Policy Across the continent* (Wiesbaden, Springer VS, 2013) 207.

8 Geciteerd in G. Simons, 'Perception of Russia's Soft Power and influence in the Baltic States', in: *Public Relations Review*, 41 (2015) 1-13.

9 K. Nielsen, H. Paabo 'How Russian Soft Power Fails in Estonia: Or, Why the Russophone Minorities Remain Quiescent', in: *Journal of Baltic Security*, 1 (2015) (2) 125-157.

	Estland			*Letland*			*Litouwen*		
	1934	*1989*	*2010*	*1935*	*1989*	*2010*	*1923*	*1989*	*2010*
Hoofdetniciteit	*88*	*62*	*69*	*76*	*52*	*59*	*81*	*80*	*83*
Russen	*8*	*30*	*26*	*11*	*34*	*28*	*2*	*9*	*5*
Oekraïners/ Witrussen	*-*	*5*	*3*	*2*	*8*	*6*	*-*	*3*	*2*
*Joden**	*0,4*	*0,3*	*0,1*	*5*	*1*	*0,4*	*7*	*0,3*	*0,1*
Duitsers	*2*	*0,2*	*0,1*	*3*	*0,1*	*0,2*	*4*	*0,1*	*0,1*
Polen	*-*	*-*	*-*	*3*	*2*	*2*	*3*	*7*	*6*

Tabel 1 Nationale samenstelling van de bevolking in de Baltische staten in procenten
* Joden worden in de Baltische staten als etnische minderheid gezien

We willen over het begrip hybride oorlogvoering hier niet verder uitweiden.[10] Wel willen we opmerken dat het in alle drie landen opviel dat de gesprekspartners het woord 'hybride' niet graag gebruikten. In Litouwen werd het als een *hype* ervaren en werd er veel meer op de angst voor een conventionele oorlog gewezen. Ditzelfde hoorden we ook in Estland.

Opvallend was dat Letland de Russische conventionele dreiging zelfs als zeer acuut ervaart. Wij komen later nog uitgebreid terug op de Baltische perceptie en het antwoord dat alle drie Baltische staten hierop samen met de NAVO formuleren. Hier gaat het voornamelijk om de Russische minderheden in Estland, Letland en Litouwen. Zij worden immers beschouwd als een van de doelwitten van Russische informatieoorlog en een mogelijke reden voor het Russische regime om te interveniëren, zoals dit ook op de Krim is gebeurd. Dit deel geeft daarom een korte beschouwing van deze minderheden en de houding van de verschillende landen ten aanzien van hen.

Minderheden

Minderheden in de Baltische staten waren er al voor dat de landen zo werden genoemd. Eerder in dit artikel hebben we kort geschetst dat de landen lange tijd door andere landen en etniciteiten, zoals Duitsers, Russen en Polen, werden bestuurd of overheerst. Tot op de dag van vandaag vormen bijvoorbeeld de burgers van Poolse komaf nog een minderheid in Litouwen, en in Estland en Letland bestaat er grote Russischtalige minderheid. Tabel 1 geeft een overzicht van de belangrijkste minderheden per land.

Al na de Eerste Wereldoorlog zochten veel bewoners van het voorheen tsaristische Rusland hun heil en toevlucht voor de Bolsjewieken en het Rode Leger in de Baltische staten. Tijdens en na de Tweede Wereldoorlog heeft het sovjetregime spoed gemaakt om de bezette landen te Russificeren.

Breekpunt

Bij het bestuderen van tabel 1 vallen twee zaken op. Ten eerste bestaan er duidelijke veranderingen in samenstelling van etnische groepen van voor de Tweede Wereldoorlog en tijdens de Koude Oorlog. Ook al is dat in de tabel niet geëxpliciteert, de Tweede Wereldoorlog was een duidelijk breekpunt. De joodse gemeenschap had veel te lijden van de Duitse bezetting, werd gedeporteerd en uiteindelijk in de andere 'bloedlanden' omgebracht.[11]

De joden die tijdens de sovjettijd nog in de landen woonden, hebben na de val van de Berlijnse muur hun heenkomen elders gezocht. De politieke, bestuurlijke en culturele elite in

10 Voor een indruk van Ruslands benadering van hybride oorlogvoering zie A.J.C. Selhorst 'Russia's Perception Warfare: The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine', in *Militaire Spectator* 185 (2016) (4) 148-164.

11 Een onderdeel van de reis was trouwens het bezoek aan de villa van de Wannsee-conferentie in Potsdam, waar op een gure 20 januari 1942 de 'Endlösung', de 'definitieve oplossing' voor het Jodenvraagstuk, werd besloten. Het begrip 'bloedlanden' is ontleend aan T. Snyder, *Bloedlanden* (Amsterdam, Ambo, Anthos, 2011).

deze landen, veelal uit de etnisch dominante bevolking gerekruteerd, werd in groten getale tijdens het Stalinistische regime naar Siberië gedeporteerd; een eufemisme voor een wisse dood.

Heterogene groep

Ten tweede valt uit de tabel op te maken dat de minderheden in de Baltische staten divers zijn. En ook de Russischtalige minderheid is niet een enkele groep, maar is heterogeen. Los van het feit dat er bijvoorbeeld ook Oekraïners en Wit-Russen onder vallen, zijn de bewoners van de mondaine badplaats Jurmala, vlakbij Riga, en de grote groep Russen in Riga geenszins te vergelijken met de grote, verhoudingsgewijs armere, groep van Russische komaf die aan de oostgrens van Letland woont.

Tijdens onze reis vertelden onderzoekers, vertegenwoordigers van de staten en ook Russischtaligen ons vaak dat veel Russen en Russischtaligen geen behoefte hebben om bij Rusland te horen, laat staan dat zij door 'de grote broer' bevrijd zouden willen worden. Een belangrijke factor hierbij is het lidmaatschap van de Baltische staten van de EU. Dit levert hen niet alleen economische voordelen op, maar ook op sociaal-cultureel gebied is de EU een zeer aantrekkelijk alternatief. Deze *soft power* van de EU is in het huidige, westerse EU-debat helaas onderbelicht, maar is in de Baltische staten prominent aanwezig.

Terwijl de minderheden positief zijn ten opzichte van de EU, worden zij veelal door zowel Estland als Letland tegengewerkt. Het is voor hun zeer moeilijk om het volledige staatsburgerschap in deze landen te verkrijgen.

In Litouwen speelt dit veel minder, vooral omdat dit land relatief weinig minderheden kent. Daarnaast kregen alle minderheden verhoudingsgewijs gemakkelijk het Litouwse staatsburgerschap.

Estland en Letland daarentegen sloten en sluiten veel niet-etnische Esten of Letten buiten. Stoiber en Urdze gaan zo ver om met betrekking tot de burgerrechten van een 'democratisch deficit' te spreken.[12] Dit begon al vlak na de val van de Berlijnse muur.

Door de Russische bezetting en onderdrukking werd vanaf 1990 een soms zeer exclusief en restrictief nationalistisch beleid in deze landen gevoerd, dat het verkrijgen van het staatsburgerschap tot op heden bemoeilijkt. In de eerste jaren na de onafhankelijkheid was er weliswaar nog een emigratiegolf van regimegetrouwen en militairen, maar het overgrote deel gaf er de voorkeur aan om in de Baltische staten te blijven.[13] Dit zorgt tot op heden vooral in Letland voor een steeds grotere scheefgroei, met name in de hoofdstad Riga.

Hoewel de Letten in Riga nog steeds de grootste groep vormen, verandert ook hier de samenstelling van de bevolking, mede door emigratie van etnische Letten naar andere Europese landen, steeds meer.[14] Een gevolg is de verkiezing van de eerste burgemeester in Riga met een Russische achtergrond, Nils Usakovs, in 2014. Dit is opmerkelijk, omdat de Russischtalige minderheid op nationaal niveau niet automatisch kiesrecht heeft. Een soortgelijk beleid bestaat ook in Estland, dat een vergelijkbare etnische samenstelling en vergelijkbare problemen heeft. Althans, de problemen zijn – zij het in mindere mate – net als in Letland gedeeltelijk zelf gecreëerd.

Eisen aan staatsburgerschap

Beide landen hebben met de herwonnen onafhankelijkheid tamelijk harde eisen aan het verkrijgen van hun nationaliteiten gesteld. Dit hing samen met het volkenrechtelijke standpunt dat de Baltische staten formeel nooit hebben opgehouden te bestaan, ook niet tijdens de s ovjetoverheersing. Dit standpunt wordt door veel westerse staten gedeeld. Aan de andere kant gingen de mensen die sinds 1940

12 M. Stoiber, S. Urdze, 'Beteiligungsformen ethnischer Minderheiten und demokratische Qualität in den baltischen Staten', in M. Knodt, S. Urdze (Hrsg.), *Die politischen Systeme der baltischen Staaten* (Wiesbaden, Springer VS, 2012) 189-191.

13 A. Urdze 'Minderheiten und Minderheitspolitik in den baltischen Staaten', in M. Knodt, S. Urdze (Hrsg.), *Die politischen Systeme der baltischen Staaten* (Wiesbaden, Springer VS, 2012) 201.

14 A. Urdze, 2012:201-202.

FOTO KANSELARIJ VAN DE PRESIDENT VAN LETLAND

Herdenking in Letland van het juk van de sovjetbezetting, maart 2017

naar de Baltische staten waren getrokken ervan uit dat deze zich in 1940 wel vrijwillig bij de Sovjet-Unie hadden aangesloten.[15]

Het gevolg is dat beide groepen tot op de dag van vandaag zeer stellig in hun standpunt zijn. Estland en Letland stellen eisen aan het staatsburgerschap, waaronder de beheersing van het Ests dan wel Lets, terwijl de Russischtaligen erop hameren dat zij ook zonder deze toets recht hebben op een officieel paspoort.

Mede door dit verschil in opvatting, woont in Estland een groot aantal mensen zonder een officieel paspoort en met beperkte rechten. De situatie in Estland valt verhoudingsgewijs nog mee. De steeds soepelere wetgeving en het feit dat deze groep wel veel voordelen van de EU geniet, behalve het vrije verkeer van arbeid, zorgt ervoor dat er weinig noemenswaardige spanningen ontstaan. Veel grotere problemen doen zich daarentegen voor in Letland.

Letland ontdeed zich vrij snel, en in extremere vorm dan de andere landen, van het juk van sovjetoccupatie en –kolonisatie. Toen er in 1998 – en onder druk van de Raad van Europa, de OVSE en de EU – eindelijk een oplossing kwam voor het toekennen van staatsburgerschap, had de lange periode van onzekerheid hierover al voor grote tegenstellingen gezorgd. De eis dat men de Letse taal machtig moest zijn, belangrijke episoden in de nationale geschiedenis moest kennen, evenals de constitutie en het volkslied teneinde een Lets paspoort te verkrijgen, werd door veel niet-Letten verworpen. ‘Zij voelden zich misleid,

15 A. Urdze, 2012: 202.

beledigd en gediscrimineerd'.[16] Nog in 2011 was ruim 200.000 van de in Letland wonende Russen stateloos, de zogenoemde grijze paspoorten. Zij mogen echter wel zonder visum naar Rusland reizen.[17]

Informatiecampagnes

Uiteraard probeert Poetin deze grote groepen in Estland en Letland met slimme en uitgebreide informatiecampagnes te bereiken, met als mogelijk doel de landen zo te destabiliseren. Dat gebeurt onder meer met behulp van de staatstelevisie, die door de overheid wordt beheerst. De staatstelevisie zendt vooral grote en dure shows uit, waar blijkbaar veel Russischtaligen van houden. Pogingen van Estse of Letse zijde om hier een kwalitatief hoogwaardig en informatief televisieprogramma tegenover te stellen waren al bij voorbaat gedoemd te mislukken, doordat men niet in staat was met de populaire propagandazenders uit Rusland te concurreren.[18]

Poetin heeft echter een probleem: de mensen kijken wel naar zijn televisieprogramma's, of worden via andere methodes beïnvloed, maar anders dan de overgrote meerderheid van Rusland beschouwen zij het huidige Rusland niet als heilstaat en Poetin niet als de Messias. Als het gaat om Estland vatten Nielsen en Paabo de indrukken die we kregen uitstekend samen: '*although Russia does indeed have a number of soft power resources, their potential for being translated into actual power and influence is too often exaggerated, not least because Europe provides a much more attractive focus point for the disgruntled than Moscow*'.[19] Met andere woorden, de maatschappelijke splijtzwam die Russische tv-producties willen zijn, zijn ze niet.

De meeste Russischtalige burgers zijn tevreden met de status quo en hun leven in de Baltische staten; het gras aan de andere kant is kennelijk toch niet altijd groener. Dit is ook de indruk die wij tijdens de reis kregen, niet in de laatste plaats toen we met een niet-gouvernementele organisatie spraken die zich inzet voor de integratie van de Russen in Estland, en dan vooral in de meest noordelijke stad, Narva, waar maar 5 procent van de bevolking Ests is.

Speldenprikken

De sociaaleconomische disbalans tussen Tallin en het oosten van Estland is groot, zo bleek. Toch is ook in dit deel van het land maar een klein percentage voor een nieuwe 'samensmelting' met Rusland. En ook in Letland wordt Poetin niet als grote strateeg, maar veeleer als rasopportunist gezien. Volgens een van de experts is het wel belangrijk om Poetin niet de kans te geven constant speldenprikken uit te delen. Deze speldenprikken kunnen weliswaar geen NAVO-reactie volgens artikel 5 uitlokken, maar kunnen wel tot grote ongerustheid en zorgen leiden in de Baltische staten en bij de andere NAVO-leden. Hiertoe behoort ook Ruslands opbouw van conventionele strijdkrachten. De Baltische staten en NAVO lijken zich op deze dreiging voor te bereiden.

De Baltische strijdkrachten en NAVO na 2014

Tot aan 2014 was de inzet van de verhoudingsgewijs kleine Baltische krijgsmachten in alle landen beperkt tot internationale missies, waarbij voor alle drie landen gold dat zij zich voornamelijk op het landoptreden oriënteerden. Uiteraard is de territoriale defensie voor de Baltische staten altijd van groot belang geweest, maar sinds 2014 kan duidelijk worden gesteld dat de strijdkrachten van al deze landen zich in een 'achtbaan vol veranderingen' bevinden.

Defensiebudgetten Baltische staten

Dit toont het verhoogde defensiebudget ook duidelijk aan. Estland, dat na de financieel–economische crisis van rond de 2 procent naar 1,7 procent in 2011 ging, stond in 2015 weer op 2 procent van het bbp. Letland ging van circa 1,6 procent in het begin van de jaren 2000 naar 0,9 procent, maar is nu hard bezig om binnen de komende twee jaar de norm van 2 procent te halen.

16 A. Urdze, 2012: 209. Eigen vertaling.
17 Idem.
18 Nerijus Maliukevicus 'Tools of Destabiliztion: Kremlin's Media Offensive in Lithuania', in: *Journal of Baltic Security* 1 (2015) (1) 117-124.
19 K. Nielsen, H. Paabo 2015: 125.

FOTO US ARMY, A.M. COLIN

Tallinn, Estland, 2014. Estse militairen vieren samen met NAVO-bondgenoten uit onder meer België, Polen, het VK en de VS de Estse onafhankelijkheid

Hetzelfde geldt voor Litouwen, dat voorheen altijd rond de 1 procent schommelde.[20] In 2016 heeft het land € 575,2 miljoen, oftewel 1,5 procent van het bbp voor defensie gereserveerd. Volgens eigen zeggen is dit het snelst groeiende defensiebudget van alle NAVO-landen.[21]

Gezien de relatief kleine economieën gaat het hierbij om bedragen tussen de 450 miljoen tot een kleine miljard euro (na verhoging). De landen geven daarmee duidelijk de boodschap hun veiligheid en het Atlantische bondgenootschap zeer serieus te nemen.[22] Bovendien is de 2-procent norm essentieel, indien de NAVO-landen bij de VS in een goed daglicht willen blijven staan. De huidige Amerikaanse vicepresident, Michael Richard Pence, onderstreepte dit eens temeer tijdens de Münchner Sicherheitskonferenz 2017.[23]

Inhaalslag

Ook qua materieel zijn de strijdkrachten met een grote inhaalslag bezig. Estland gebruikte in 2015 circa 118 miljoen euro, ongeveer 28,8 procent, voor de aanschaf van wapens.[24] Letland wil tot 2018 meer dan 20 procent van de defensiebegroting gebruiken voor investeringen[25] en Litouwen wilde in 2016 34,3 procent besteden aan wapens en groot materieel.[26]

20 Alle cijfers zijn afkomstig van https://www.sipri.org/databases/milex. Daarnaast is gebruik gemaakt van cijfers die experts en ambtenaren in de Baltische staten noemden tijdens persoonlijke gesprekken.

21 Zie: http://kam.lt/en/budget_1065.html.

22 In Berlijn nam een gesprekspartner ons mee in een interessant gedachte-experiment door ons voor te stellen dat Duitsland met een bbp van circa 3,4 biljoen (3.400 miljard) aan de 2- procent norm zou voldoen. Uitgedrukt in dollars ligt het Duitse bbp een kleine biljoen hoger dat van Frankrijk en het VK. Zie: https://www.google.nl/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_mktp_cd&idim=country:DEU:FRA:GBR&hl=nl&dl=nl met gegevens van Wereldbank.

23 Zie: https://www.whitehouse.gov/the-press-office/2017/02/18/remarks-vice-president-munich-security-conference.

24 Zie: http://www.kaitseministeerium.ee/en/objectives-activities/defence-budget.

25 Zie: http://www.mod.gov.lv/Par_aizsardzibas_nozari/Politikas_planosana/Vald_prioritaspx.

26 Zie: http://kam.lt/en/budget_1065.html.

BRON: NAVO

De Enhanced Forward Presence van de NAVO in Polen en de Baltische staten, maart 2017

Samen met de NAVO werken de landen aan een vorm van afschrikking met een bepaalde mate van 'gevoeligheid voor het veiligheidsdilemma': in plaats van de 10.000 door Polen geëiste troepen[27] werkt het bondgenootschap aan verschillende concepten. Deze concepten beogen enerzijds de Baltische staten en Polen gerust te stellen, en anderzijds Rusland niet onnodig provoceren. Tijdens de top in Wales in 2014, besloot de alliantie als reactie op de groeiende instabiliteit langs haar grenzen om het *Readiness Action Plan* (RAP) te implementeren. Hierop voortbouwend werd tijdens de top van Warschau in 2016 besloten tot de *tailored forward presence* met een multinationale framework brigade in Roemenië en de *enhanced forward presence* (eFP) in de Baltische staten en Polen.

De oprichting van de eFP geschiedt ook uit strategische noodzaak. In het begin van 2016 verscheen een kritisch rapport van RAND over de geostrategische ligging van de Baltische staten en hoeveel moeite het de NAVO zou kosten om deze met conventionele middelen te verdedigen. Volgens een serie *wargames* in 2014 en 2015 zou het maximaal 60 uur duren voordat Rusland de Baltische staten volledig onder de voet loopt.[28]

Opbouw Russische strijdkrachten

Om en nabij de Baltische staten en niet in de laatste plaats in Kaliningrad, zijn de Russen bezig veel conventionele strijdkrachten te plaatsen. Maar niet alleen de aantallen, ook de kwaliteit van de bewapening blijkt indrukwekkend. Zo beschikt Rusland over artilleriestukken en raketartillerie, die een reikwijdte hebben van respectievelijk 29 en 90 km. Uiteraard schiet de PzH2000 verder dan de Russische stukken, maar qua aantallen is de NAVO ver verwijderd van Rusland. Bovendien bezitten de Russen in grote getallen (thermobarische) clustermunitie.[29] Vooral dit laatste geeft ze een grote voorsprong tegen oprukkende NAVO-tanks en infanterie.

Daarnaast draagt de enorme Russische wapenopbouw langs de Baltische staten ertoe bij dat het luchtruim superioriteit heeft.

27 Zie: http://www.telegraph.co.uk/news/worldnews/europe/ukraine/10737838/Ukraine-crisis-Poland-asks-Nato-to-station-10000-troops-on-its-territory.html.

28 D.A. Shlapak, M.W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (RAND Corporation 2016).

29 David A. Shlapak en Michael W. Johnson op Zie: https://warontherocks.com/2016/04/outnumbered-outranged-and-outgunned-how-russia-defeats-nato/; https://www.washingtonpost.com/opinions/global-opinions/russias-superior-new-weapons/2016/08/05/e86334ec-08c5-11e6-bdcb-0133da18418d_story.html?utm_term=.2ef5e6b93372; Zie: https://en.wikipedia.org/wiki/List_of_equipment_of_the_Russian_Ground_Forces#Self-propelled_artillery.

Russia fields perhaps the most formidable array of surface-to-air missile (SAM) defenses in the world. Operating from locations within Russian territory, these SAMs far outrange existing defense-suppression weapons and present a credible threat to U.S. and allied airpower that would be costly and time-consuming to counter.[30] Bovendien bereiken de in Kaliningrad gestationeerde Iskanderraketten, die ook nucleair kunnen worden bewapend, bijna alle hoofdsteden van de Baltische landen.[31]

Opties voor de NAVO

Voor de NAVO resteren daarbij enkel 'slechte opties': *a bloody counter-offensive, fraught with escalatory risk, to liberate the Baltics; to escalate itself, as it threatened to do to avert defeat during the Cold War; or to concede at least temporary defeat, with uncertain but predictably disastrous consequences for the Alliance and, not incidentally, the people of the Baltic*.[32] Maar, met zeven brigades, waarvan drie ' zwaarbewapend', kan men de Russen wel afschrikken, aldus het RAND-rapport. De jaarlijks kosten hiervoor zouden dan wel 2,7 miljard US dollar bedragen.[33] Al met al leidt de Russische bewapening ertoe dat de Baltische staten voor het Westen een *no-go area* worden. Toch probeert het westerse bondgenootschap hierop een antwoord te formuleren.

'Framework nations'

Onder de hoede van vier *framework nations* – Canada, Duitland, Verenigd Koninkrijk en de VS – worden vier multinationale bataljons gestationeerd in respectievelijk Letland, Litouwen, Estland en Polen. De functie van deze bataljons is de sterke Transatlantische band te

30 D.A. Shlapak, M.W. Johnson op: warontherocks.com.
31 Dus ook Berlijn, Warschau, Stockholm, Helsinki en Kopenhagen. Zie: http://www.spiegel.de/politik/ausland/russland-polen-und-litauen-fuerchten-iskander-raketen-nahe-eu-grenze-a-1115810.html.
32 David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (RAND Corporation 2016), 1.
33 Idem, 1-2.

Nederland levert vier F-16's ter verdediging van het luchtruim boven de Baltische staten. Een vlieger controleert de bewapening van zijn F-16, januari 2017

FOTO MCD, G. VAN ES

demonstreren, *'and making clear that an attack on one Ally would be considered an attack on the whole Alliance'*.[34] Met andere woorden, de bataljons onderstrepen dat artikel 5 van het NAVO-verdrag geen holle kreet is. Deze bataljons zijn een belangrijk signaal in de richting van Moskou. Nederland heeft in het voorjaar van 2017 een compagnie geplaatst in Litouwen. In totaal worden er 270 militairen geplaatst, inclusief Boxer-pantserwielvoertuigen en CV90-infanteriegevechtsvoertuigen.[35]

De Baltische staten reageren overwegend positief op de komst van eFP. Een vooraanstaande veiligheidsexpert in Litouwen gaf duidelijk aan dat men zeer blij was met de komst van de Duitsers en Nederlanders, die als belangrijke en betrouwbare partners te boek staan. Een andere gesprekspartner stelde dat de bereidheid van NAVO-militairen om zich mogelijk op te offeren goed is voor het Baltische moreel. Bovendien is de gedachte in de Baltische staten dat het de relatie met Rusland juist bevordert. Volgens een Litouwse *official* is Rusland pragmatisch en kan er goed mee worden samengewerkt, mits de krachtsverhouding evenwichtig is. Ook hier werd Poetin als opportunist gezien, die zo ver gaat als het bondgenootschap hem laat gaan.

Voor sommigen gaat de opbouw van de NAVO-aanwezigheid niet snel genoeg. Vooral in Letland en Litouwen, waar men volgens de gesprekpartners een acutere dreiging voelt, is men bang dat Rusland iets gaat proberen voor dat de NAVO-eenheden paraat zijn. Deze gereedheid wordt in de loop van het voorjaar 2017 bereikt.

Garantie van de NAVO

Tot die tijd bestaat de belangrijkste garantie die de NAVO te bieden heeft uit de *Very High Readiness Joint Task Force* (VJTF) en *NATO Force Integration Units* (NFIU). Als reactie op Ruslands optreden in Oekraïne werd in 2014 besloten de NATO Response Forces door deze snel verplaatsbare eenheden te versterken. Dit omvat ook een multinationale brigade met 5000 militairen. Deze eenheid dient als bruggenhoofd voor de *follow on forces*. Wij zijn, mede door de mogelijkheden van Rusland om het zee- en luchtruim vanuit Kaliningrad te beheersen, echter somber gestemd over de inzetkansen voor deze eenheden.

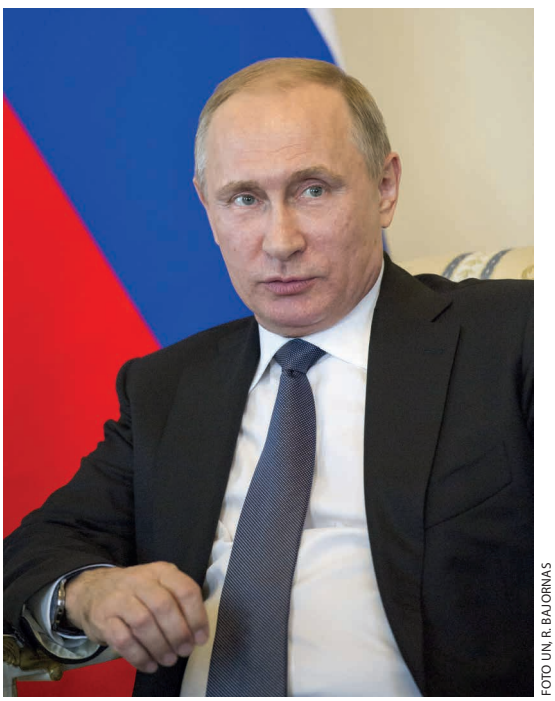


FOTO UN, R. BAJORNAS

President Poetin tracht de Russische minderheden op verschillende manieren voor zijn karretje te spannen

Goede, maar kleine strijdkrachten en een verdeelde NAVO

Het is een feit dat de NAVO en vooral de VS belangrijk zijn voor de veiligheid van de Baltische staten. Tegelijkertijd werd ons duidelijk dat ook de EU een belangrijke rol speelt. Zij biedt niet alleen economische welvaart, maar is tevens een aantrekkelijk alternatief voor Rusland, niet alleen voor de minderheden in de Baltische staten. Wij constateren echter dat er op dit moment nog niet geen effectieve gezamenlijke militaire afschrikking bestaat, noch een afgestemde (communicatie)strategie.

34 Zie: http://www.nato.int/cps/en/natohq/topics_136388.htm?selectedLocale=en.

35 Zie: https://www.defensie.nl/actueel/nieuws/2017/03/23/hoofdmacht-naar-litouwen.

Vraagtekens
De effectiviteit van de VJTF valt te betwijfelen, omdat de Russische opbouw van wapens de daadwerkelijke inzetbereidheid van de NAVO-strijdkrachten voor de verdediging van de Baltische staten bijna onwaarschijnlijk maakt. Dit komt doordat het Russische militaire overwicht zo groot is dat het verplaatsen van de VJTF verhoudingsgewijs gemakkelijk kan worden tegengehouden.

Daarnaast delen we de zorgen van sommige experts dat er in de betrokken NAVO-landen verschillende ideeën bestaan over de daadwerkelijk inzet van troepen tegen Rusland. Ietwat gechargeerd werd gesteld dat de landen door hun deelname aan eFP en VJTF de bereidheid tonen om te vechten, maar dat men vraagtekens plaatst bij de bereidheid van de NAVO om bij een Russische inval daadwerkelijk artikel 5 in werking te stellen. Men mag bovendien niet vergeten dat er in sommige NAVO-landen leiders aan de macht zijn die steeds meer naar Rusland trekken. Hiertoe behoren Bulgarije, Turkije – zie de verrassende toenadering in het Syrië-conflict – en wellicht zelfs de VS.[36]

Het Rusland van Poetin heeft in Estland (2007), Georgië (2008), en de Krim en Oekraïne (2014) laten zien juist de Russische minderheden in deze landen voor zijn karretje te willen spannen. Dit deed Rusland met respectievelijk cyberstrategieën, het gebruik van de NAVO- communicatiestrategie uit Kosovo en (semi) officiële troepen. Dit is ook een belangrijke factor in de Gerasimov-doctrine.[37] Ondanks dat er tot op de dag van vandaag problemen bestaan met de Russischtalige minderheden in de Baltische staten, achten wij het minder waarschijnlijk dat zij actief zullen meewerken aan een interventie door Rusland.

Niet elke in de Baltische staten woonachtige Russischtalige is onderdeel van de vijfde colonne van Moskou, zoals we hopelijk hebben laten zien. Integendeel: onze indruk, die de literatuur mede bevestigt, is veeleer dat de Russischtalige minderheid zeer pragmatisch het beste van beide werelden aanvaardt. Als puntje bij paaltje komt, kiest de overgrote meerderheid waarschijnlijk voor het Westen.

Europa: een aantrekkelijk alternatief
Bij alle negatieve kritiek op de EU in het afgelopen decennium vergeten we maar al te snel dat Europa nog steeds veel aantrekkelijks te bieden heeft. Dit is zeker waar als men Europa vergelijkt met de levensstandaard in Rusland en in de vele voormalige sovjet-deelrepublieken.

De EU is voor veel Russischtaligen aantrekkelijker dan Poetin

Het leven van de minderheden in de Baltische staten mag dan niet overdadig zijn, maar vergeleken met de minder dan € 139,- per maand die 19,4 procent van de Russische bevolking ter beschikking heeft, en daarmee onder de armoedegrens leeft, gaat het nog goed.[38]

Communicatie en propaganda
Het blijft wel nodig dat het westen zijn aantrekkelijkheid in de ogen van de Russischtalige minderheid behoudt en dit ook succesvol blijft communiceren. Dat is waarschijnlijk het belangrijkste wapen dat men tegenover het rijk van Poetin kan inbrengen. Mede daarom is het goed dat het NAVO STRATCOM Centre of Excellence in Riga zit, ook al was Ruslands informatieoorlog niet de directe aanleiding.[39]

36 Zie: http://www.spiegel.de/politik/ausland/bulgarien-rumen-radew-zum-praesidenten-gewaehlt-a-1121095.html. De rol van de VS blijft onduidelijk. Tijdens het schrijven van dit artikel in maart 2017 was er een officieel onderzoek in de VS gaande naar de contacten tussen het verkiezings- en latere regeringsteam van Trump en Rusland.

37 A.J.C. Selhorst, 'Russia's Perception Warfare: The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine', in: *Militaire Spectator* 185 (2016) (4) 148-164.

38 Zie: https://www.theguardian.com/world/2016/mar/22/millions-more-russians-living-in-poverty-as-economic-crisis-bites. Zie ook J.C. Lee 'When the Russian Economy Is Tumbling', *New York Times*, Late Edition (East Coast) [New York, N.Y] 14 Apr 2016: A.8. Het Baltische land dat de grootste problemen heeft, vooral na de financieel-economische crisis van 2008, is Litouwen. Dit land had verreweg de kleinste groep Russen als minderheid. Vergelijk: B. Gruževskis, I. Blažiene Die wirtschaftliche und soziale Lage in den Baltischen Staaten: Litauen. (Studie Europäischer Wirtschafts- und Sozialausschuss), 2013.

39 De aanleiding voor het oprichten van STRATCOMCOE vormde de slechte communicatiestrategie van de NAVO in Afghanistan.

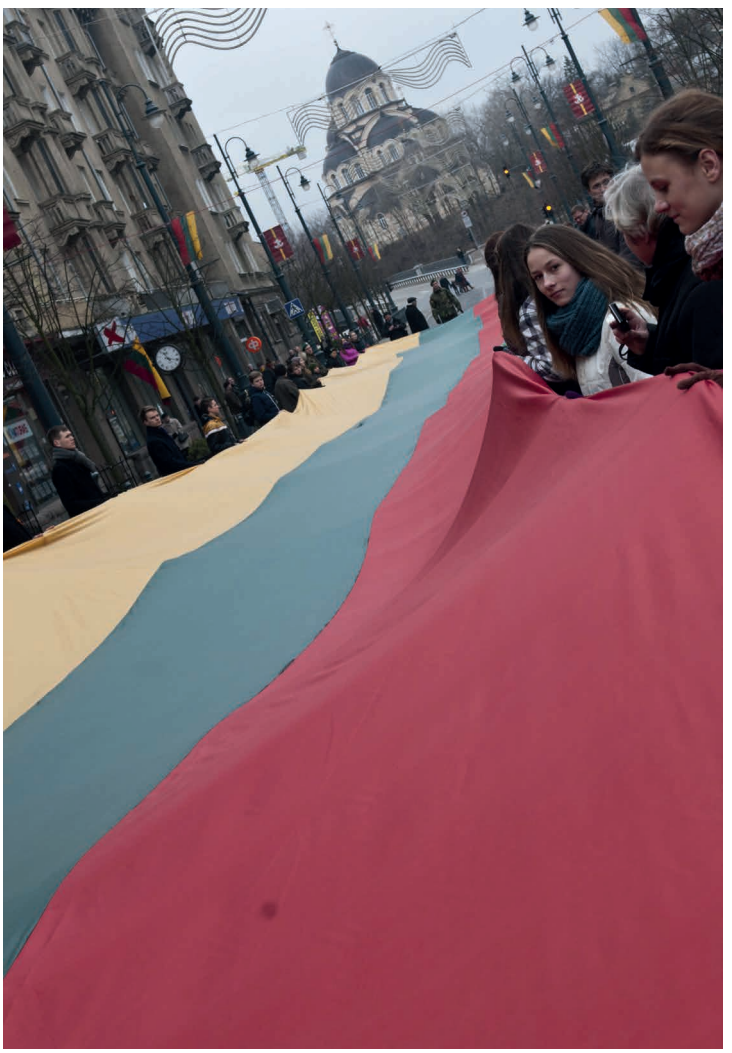


FOTO US ARMY, M. LEUCK

Litouwse burgers en militairen dragen een 200 meter lange Litouwse vlag ter ere van de onafhankelijkheid van hun land, Vilnius, 2015

Tijdens ons bezoek kregen we de indruk dat dit centrum door de Letten omarmd wordt, getuige de investeringen die men maakt en de status die door de benoeming van een voormalig staatssecretaris als directeur aan het centrum wordt gegeven en een actieve staatssecretaris als hoofd van het bestuurscomité. De belangrijkste taak van het centrum is het ontleden van de communicatiestrategieën van de tegenstanders, niet alleen Rusland.[40]

40 Zie: http://www.stratcomcoe.org.

Van effectieve counterstrategieën is echter nog geen sprake. Dit komt mede door de verschillende nationale benaderingen en strategieën. Daarnaast begrepen we van een vooraanstaande expert op het gebied van Russische informatieoorlogvoering dat de propagandapraktijken van het Kremlin met het werk van illusionisten kan worden vergeleken.

Mede door enorme investeringen in de propagandamachine, volgens een van onze gastsprekers een geschatte € 300 miljoen, weet Rusland de westerse media herhaaldelijk op hun zwakste plek te raken. Voorbeelden zijn er ten over. Vooral wanneer de Russische berichtgeving klakkeloos door westerse media wordt overgenomen. Daarnaast herinneren zich de meeste Nederlanders zich nog levendig de verschillende Russische versies van het neerstorten van vlucht MH17. Naast Ruslands militaire optreden, zet ook dit de relaties met het Westen herhaaldelijk onder druk.

Conclusie

In dit artikel stond de vraag centraal of de Baltische staten en hun Russische minderheden voor de NAVO een veiligheidsprobleem zijn. Wij constateren dat er vooral in Estland en Letland grote groepen Russischtalige minderheden wonen, maar dat zij zich veel minder voor het propagandakarretje van Poetin laten spannen dan de minderheid in Oekraïne. Tegelijkertijd zagen we dat op dit moment vooral Letland en Litouwen de Russische militaire dreiging als meest acuut ervaren.

Wij concluderen dan ook dat de Russische conventionele troepenopbouw de grootste bedreiging vormt voor deze landen en de NAVO. Wil de NAVO ernst maken met het verdedigen van het bondgenootschap, dan moet ze met name tegen Rusland snel, adequaat en vooral eensgezind optreden. De VJTF, NFIU en eFP zijn een goed begin, maar het blijft belangrijk dat de alliantie gezamenlijk doelen tegenover Rusland blijft formuleren en nastreven. Of dit zo blijft is, mede gezien de pro-Russische toon in sommige lidstaten, zeer de vraag. ■

Technologische innovaties voor de militaire gezondheidszorg

'Telehealth' voor virtuele consultatie tijdens missies, ondersteuning van militair artsen met behulp van 'augmented reality', of vroegtijdige bloedstolling bij letsel met behulp van nanomedicine. Deze technologische innovaties kunnen bijdragen aan het behoud en de bevordering van de gezondheid en aan een optimale inzetbaarheid van de militair. Dit artikel beschrijft meerdere medisch relevante technologische toepassingen aan de hand van vier categorieën: Sensoring & Monitoring, Robotica & Artificial Intelligence, Genomica & Biotechnologie, en Nanomedicine. Eerst komt de vraag aan de orde welke ontwikkelingen, zowel civiel als operationeel, de behoefte aan technologische ontwikkelingen voeden. Vervolgens worden de vier categorieën en subcategorieën uiteengezet, met inbegrip van concrete toepassingen en voorbeelden uit de praktijk. Het doel van dit artikel is bewustwording creëren van de mogelijkheden en – soms – risico's van technologische ontwikkelingen binnen het 'human domain' die relevant zijn voor de militaire gezondheidszorg.

*D.J. Siemerink, MSc**

Een van de taken van de Militaire Gezondheidszorg (MGZ) is het leveren van operationele geneeskundige ondersteuning.[1] Hierbij streeft men naar een hoogwaardige kwaliteit van zorg die, ook onder operationele omstandigheden, afgestemd is op civiele kwaliteitsnormen. Tijdens multinationale operaties dient men tevens te voldoen aan de NAVO-richtlijnen voor tijdige en adequate hulpverlening en afvoer van gewonden.[2]

Veranderingen in operationele omstandigheden zorgen voor toenemende complexiteit bij zorgverlening tijdens missies. Concrete voorbeelden hiervan zijn het expanderende en moeilijker begaanbaar wordende voorterrein bij grootschalig optreden, de toename van kleinschalige operaties (*light footprint operations* - LFO), urbanisatie en hybride oorlogvoering. De inzet van uitgebreide medische voorzieningen is in deze gevallen niet altijd haalbaar. Daarnaast zorgt de dynamiek in dimensies en domeinen van oorlogvoering voor een toename van de complexiteit.

Maatregelen die zijn gericht op het bevorderen en behouden van de gezondheid en inzetbaarheid worden steeds meer beschouwd als onderdelen van het omvangrijke *human domain*. Technologische ontwikkelingen en hyper-

* De auteur heeft Biomedical Engineering gestudeerd aan de Universiteit Twente en is werkzaam als adviseur Innovatie op het gebied van medische techniek bij de afdeling Strategische Militaire Gezondheidszorg van de Staf DGO.

1 Blauwdruk Militaire Gezondheidszorg 2015, 'Zorg voor inzetbaarheid, inzet voor zorg', 1 augustus 2011.

2 R. Hoencamp, 'Afghanistan 2006-2010: medical aspects and challenges', in: *Task Force Uruzgan* (2015).

FOTO US ARMY S. REEL

Telemedicine, oftewel zorg op afstand, wordt al bijna honderd jaar toegepast in de gezondheidszorg

connectiviteit voeden het belang van het *cyber domain* en de beheersing van het elektromagnetisch spectrum.[3] Deze spelen ook binnen de MGZ een steeds grotere rol met de digitalisering van de gezondheidszorg.

De veranderingen vormen een uitdaging als het gaat om het voldoen aan de doelstelling van kwalitatief hoogwaardige gezondheidszorg leveren. Het vergt adaptiviteit en flexibiliteit om te kunnen anticiperen op deze veranderende omstandigheden en om aan de gevarieerde zorgvraag te kunnen voldoen. Dit artikel beschrijft hoe verschillende technologische innovaties hierin een rol kunnen gaan spelen.

Civiele ontwikkelingen

De MGZ wordt, naast verandering in operationele omstandigheden, ook beïnvloed door civiele ontwikkelingen. Deze kunnen bijdragen aan het consolideren en bevorderen van de kwaliteit van de zorg. Dit maakt Defensie een aantrekkelijke en progressieve werkgever, wat de continue uitwisseling van medisch personeel met de civiele arbeidsmarkt kan stimuleren. De gezondheidszorg wordt steeds meer als een continuüm beschouwd van gezondheidsbevordering en ziektepreventie, waarbij de patiënt centraal staat.

Gezondheid kan volgens Machteld Huber het best beschreven worden als *'het vermogen om zich aan te passen en een eigen regie te voeren, in het licht van de fysieke, emotionele en sociale uitdagingen in het leven'*.[4] Door toenemende connectiviteit kan er meer medische data door de patiënt ontsloten worden. Dit vergroot de zelfredzaamheid, de regie en de zelfzorg van patiënten, wat overigens ook wordt gestimu-

3 Land-Warfare-Centre. Editie Silene - Deducties voor het landoptreden. Utrecht: Afdeling Land Warfare, 2015.

4 M.A.S. Huber, 'Towards a new, dynamic concept of Health: Its operationalisation and use in public health and healthcare and in evaluating health effects of food', Proefschrift Universiteit Maastricht (2014).

leerd vanuit de overheid.[5] Dit artikel beschrijft toepassingen die bijdragen aan het optimaal benutten van medische data en die inzicht geven in de gezondheid en inzetbaarheid van de militair.

Naast mogelijkheden ook risico's

De categorisering van de toepassingen zoals gebruikt in dit artikel, is vooral bedoeld om een overzicht te geven en sluit een overlap of samenhang niet uit. Veel toepassingen zullen elkaars ontwikkeling en functioneren namelijk versterken, wat een exponentiële technologische groei kan veroorzaken. Niet meegaan in deze ontwikkeling betekent al snel een onacceptabele achterstand. Wanneer opponenten technologische innovaties toepassen, kan men hierdoor verrast worden. Om dreigingen te kunnen onderkennen, is het immers van belang om te weten welke ontwikkelingen gaande zijn en waar kennis en kunde te behalen valt. Dit artikel beoogt bij te dragen aan het ontsluiten van kennis over toepassingsmogelijkheden en risico's van medisch technologische ontwikkelingen.

Sensoring & Monitoring

Telemedicine

Het concept *telemedicine* wordt inmiddels al bijna honderd jaar toegepast in de dagelijkse gezondheidszorg.[6] De letterlijke betekenis van het begrip telemedicine is: *'healing at a distance'*, oftewel zorg op afstand.[7] Volgens de Nederlandse Technische Afspraak (NTA) gaat het om een telemedicine toepassing wanneer een proces in de gezondheidszorg voldoet aan twee voorwaarden:

1) afstand wordt overbrugd met behulp van ICT;
2) waarbij minstens twee personen betrokken zijn en tenminste één van hen geregistreerd staat als zorgprofessional of handelt in opdracht van een geregistreerd zorgprofessional.[8]

De ruimte die deze definitie biedt, zorgt ervoor dat er veel medisch technologische toepassingen behoren tot deze categorie. Bijvoorbeeld het verzenden van patiëntgegevens vanuit een ambulance naar een zorginstelling,[9] of het verzenden van sensordata vanuit de thuissituatie van een patiënt naar een zorgprofessional.[10]

Dankzij teleconsulting kan een militair tijdens missies in contact zijn met elke medisch specialist – zonder locatiebeperking

Een relevante toepassing van telemedicine voor de MGZ is *teleconsulting*, waarbij een virtueel consult plaatsvindt tussen medisch specialist en patiënt met behulp van ICT. Dankzij deze technologie kan een militair tijdens missie worden voorzien van een hoge kwaliteit zorg, doordat men in contact kan worden gebracht met elke medisch specialist zonder locatiebeperking. Uiteindelijk verhoogt dit dus de kwaliteit van de MGZ en bevordert dit de gezondheid en daarmee de inzetbaarheid van de militair.

Het teleconsult concept wordt al sinds 2014 toegepast in de Amerikaanse krijgsmacht.[11] Een concreet voorbeeld hiervan is het *telehealth* programma, dat is opgestart om Amerikaanse militairen die in Europa zijn te werk gesteld te voorzien van optimale zorg met behulp van virtuele consultatie.[12]

5 J. Krijgsman, 'E-Health Monitor 2016', Nictiz (2016).
6 S. Tachakra, 'Mobile e-health: the unwired evolution of telemedicine', *Telemedicine Journal and E-health* (2003) 9(3): p. 247-257.
7 S. Sood 'What is telemedicine? A collection of 104 peer-reviewed perspectives and theoretical underpinnings', *Telemedicine and e-Health* (2007) 13(5): 573-590.
8 Nederlandse Norm, 'Medische Informatica - Kwaliteitseisen telemedicine', NEN-8028:2011 (2011).
9 L. Yperzeele, 'Feasibility of AmbulanCe-Based Telemedicine (FACT) Study: Safety, Feasibility and Reliability of Third Generation In-Ambulance Telemedicine', in *PLOS ONE* (2014).
10 B.H. Dobkin, 'The Promise of mHealth: Daily Activity Monitoring and Outcome Assessments by Wearable Sensors', in *Neurorehabil Neural Repair* (2011) 25 (9) 788–798.
11 Army Medicine, 'The power of virtual health' (2016), http://armymedicine.mil/Pages/telehealth.aspx.

FOTO US AIR FORCE, W. FARNSWORTH

Het monitoren van vitale parameters, zowel operationeel als regulier, kan ertoe leiden dat er eerder maatregelen worden genomen die de gezondheid bevorderen. Hiermee kan uitval worden gereduceerd en de inzetbaarheid worden verhoogd

Portable diagnostiek

De eerder beschreven veranderende inzet zorgt voor een grotere behoefte aan zorgprocessen rond de *point of injury* (POI). Dit vergt echter flexibele en mobiele medische voorzieningen. De prioriteit daarbij is om kwalitatief hoogwaardige diagnostische middelen zo dicht mogelijk bij de POI in te zetten. Hiermee kan sneller, betrouwbaarder en nauwkeuriger een diagnose worden gesteld, waarmee een betere inschatting kan worden gemaakt van de situatie van de patiënt.

Uiteindelijk zorgt dit voor efficiëntere afhandeling van gewonden, waarmee de kwaliteit van de geleverde zorg en de inzetbaarheid van de militairen toeneemt en de kosten afnemen. Concrete toepassingen hiervan zijn: *portable monitoring* systemen voor het continu zichtbaar maken van vitale parameters; draagbare tests voor bloedanalyse, bijvoorbeeld met betrekking tot CBRN[13] dreigingen; en *portable ultrasound* systemen waarmee kwalitatief hoogwaardige diagnostiek kan worden verricht.[14]

Deze toepassingen vergen minimale middelen, zoals een portable ultrasound systeem, dat gebruik maakt van een echosonde gekoppeld aan een smartphone-applicatie.[15] De portable ultrasound systemen kunnen echter de kwaliteit en efficiëntie van de zorg in een role 0/1 of tijdens een Medische Evacuatie (MedEvac) verhogen en meer gedetailleerde inzichten geven in de situatie van de patiënt in vergelijking tot de stethoscoop.[16] Verschillende vormen van deze systemen worden al sinds

12 S. Garner, 'Telehealth Brings Long Distance Specialists to You', in U.S. Army, 15 januari 2015, Zie: https://www.army.mil/article/141020/Telehealth_Brings_Long_Distance_Specialists_to_You/.

13 Dreigingen met betrekking tot Chemische, Biologische, Radiologische of Nucleaire stoffen.

14 A.W. Kirkpatrick, 'Introduction to the use of ultrasound in critical care medicine', in *Crit Care Med* (2007) 35 (5) 290-S304. C.L. Moore, 'Point-of-care ultrasonography', in *New England Journal of Medicine* (2011) 364 (8) 749-757.

15 Aditi Pai, 'Philips launches FDA-cleared smartphone-connected ultrasound device', 23 november 2015. Zie: http://www.mobihealthnews.com/48756/philips-launches-fda-cleared-smartphone-connected-ultrasound-device/.

2009 door Amerikaanse *Special Forces medics* gebruikt en hebben hun toegevoegde waarde voor de operationele MGZ bewezen.[17]

Wearables

Zoals eerder beschreven is er een trend waarneembaar binnen de gezondheidszorg waarbij de patiënt regisseur wordt van de eigen gezondheid.[18] Door *the internet of things* heeft de patiënt continu toegang tot medische kennis die voorheen voornamelijk tijdens een bezoek aan een medisch specialist werd verkregen.[19] Daarnaast spelen commerciële partijen in op deze trend van zelfregie door producten aan te bieden die mensen in staat stellen om op eenvoudige wijze de eigen fysiologische parameters te kunnen monitoren.

Deze *Body Area Network* (BAN) technologie is opgebouwd uit een draadloos netwerk van sensoren, bedoeld om fysiologische en vitale parameters te monitoren, met als oogmerk bevordering van de gezondheid.[20] Hiertoe behoren ook *track & trace* applicaties die binnen de MGZ een bijdrage kunnen leveren aan een efficiëntere gewondenafvoer en -overdracht. Er is echter ook kritiek en discussie over de validiteit, betrouwbaarheid en effectiviteit van deze BAN's of *wearables*, die grotendeels afhankelijk is van de kwaliteit van het apparaat, maar ook van de toepassing door de gebruiker.[21]

Het gebruik van valide en betrouwbare wearables bij de individuele militair kan bijdragen aan inzicht in diens inzetbaarheid. Ook kan het monitoren van vitale parameters, zowel operationeel als regulier, het nemen van preventieve gezondheidsmaatregelen bevorderen. Hiermee kan uitval worden gereduceerd en dus de inzetbaarheid worden bevorderd. Toch zal de organisatie zich ook bewust moeten zijn van de uitdaging die er ligt op het gebied van integriteit en omgang met privacygevoelige data. Wanneer hier echter eenduidige intenties en onderbouwde argumenten voor worden vastgelegd, zou dit een toepassing mogelijk moeten maken die voor zowel werkgever als werknemer een toegevoegde waarde heeft.

FOTO US MARINE CORPS, A. SOTO-DELGADO

Bij het opleiden van jonge militaire artsen maakt men vooral in de VS vaak gebruik van 'augmented reality'-technologie. Hierbij kunnen artsen 'meekijken' met een operatie door de ogen van een medisch specialist of zelf virtueel een chirurgische ingreep uitvoeren

Augmented Reality

Als het gaat om het optimaal voorbereiden van militair artsen en verpleegkundigen kan en moet er altijd naar verbetering worden gestreefd. Naast de stressvolle operationele omstandigheden heeft men tijdens een missie te maken met een specifieke patiëntengroep, die afwijkt van de groep patiënten die men tijdens civiele stages tegenkomt. Militair artsen vertrouwd laten raken met complexe gevechtsverwondingen is dan ook een essentieel onderdeel van het opleiden.

16 F. Al, Fakoya, 'Ultrasound and stethoscope as tools in medical education and practice: considerations for the archives', in *Advances in Medical Education and Practice* (2016) (7) 381-387.

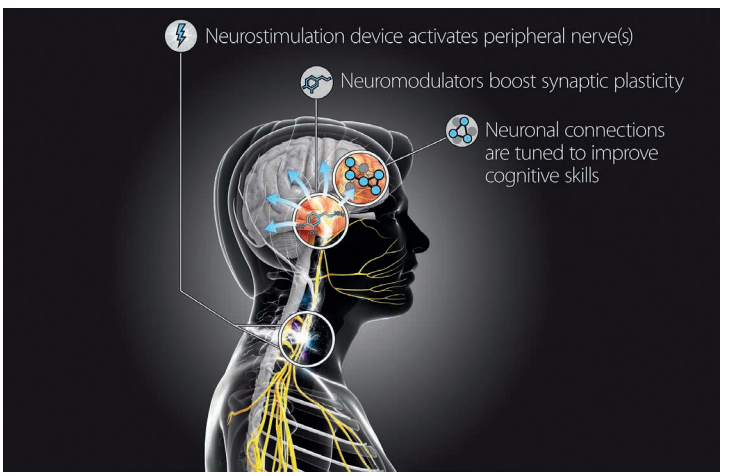
17 J.D. Crisp, 'Portable ultrasound empowers Special Forces medics', 3 februari 2010. Zie:, https://www.army.mil/article/33923/portable-ultrasound-empowers-special-forces-medics.

18 J. Krijgsman, 'E-Health Monitor 2016', in *Nictiz* (2016).

19 J. A. Diaz, 'Patients' Use of the Internet for Medical Information', in *Journal of General Internal Medicine* (2002) 17 (3)180-185.

20 Min Chen, 'Body Area Networks: A Survey', in *Mobile Networks and Applications* (2011) 16 (2) 171-193.

21 J. Jacobs, 'Blog: allemaal rotzooi, die consumenten wearables', SmartHealth 22 maart 2016, http://www.smarthealth.nl/Blog:-allemaal-rotzooi-die-consumenten-wearables. H. Murakami, 'Accuracy of Wearable Devices for Estimating Total Energy Expenditure', in *JAMA Internal Medicine* (2016) 176 (5) 702-203. K.R. Evenson, 'Systematic review of the validity and reliability of consumer-wearable activity trackers', in *International Journal of Behavioral Nutrition and Physical Activity* (2015) 12:159.



BRON: DARPA

De laatste jaren is er ook veel onderzoek naar het psychisch functioneren en vooral naar de wijze waarop hersenactiviteit kan worden gemeten en beïnvloed

In het huidige systeem oefenen jonge militaire artsen hun chirurgische capaciteiten voornamelijk met burgers, waarbij verwondingen vaak verschillen van militaire gevechtsverwondingen.[22] Bij het opleiden van civiele medisch specialisten maakt men inmiddels gebruik van *virtual* of *augmented reality*-technologie. Hierbij kunnen artsen-in-opleiding meekijken met een operatie 'door de ogen' van de uitvoerend medisch specialist, of zelf een virtuele chirurgische ingreep uitvoeren.[23] De ervaring die een medisch specialist in opleiding zo opdoet, draagt bij aan de *situational awareness* die benodigd is voor het uitvoeren van een complexe chirurgische ingreep.

Daarnaast wordt er onderzoek gedaan naar de mogelijkheden met augmented reality ter ondersteuning van de uitvoerend arts. Een voorbeeld hiervan is het gebruik van de Microsoft Hololens tijdens neurochirurgie.[24] Hierbij kunnen dieper gelegen hersenweefsels virtueel zichtbaar worden gemaakt zonder dat daarbij het weefsel hoeft te worden aangetast.

Augmented reality technologie is daarmee niet alleen van toepassing voor opleiding en training, maar kan ook dienen ter ondersteuning van een uitvoerend medisch specialist. Deze technologie biedt daarmee mogelijkheden om tijdens uitdagende operationele omstandigheden kwalitatief hoogwaardige zorg te leveren. Toepassingen van augmented reality beschouwt de Amerikaanse krijgsmacht als technieken die de kwaliteit bevorderen, zoals het rapport van het TATRC beschrijft.[25]

Robotica & AI

Human enhancement

Menselijke fysiologische capaciteiten zijn grotendeels afhankelijk van genetische eigenschappen en leefstijl-factoren. Deze capaciteiten kunnen gedeeltelijk worden gemanipuleerd met behulp van technologische toepassingen. Hierbij kan gedacht worden aan *ex vivo* middelen die de anatomische structuren van de mens kunnen ontlasten. Een exoskelet bijvoorbeeld, stelt militairen in staat om grotere afstanden af te leggen met zwaardere bepakking, met minder inspanning en een kleinere kans op blessures.

Naast *ex vivo* zijn er ook *in vivo* mogelijkheden voor uitbreiding of vergroting van menselijke capaciteiten. Hierbij zijn er toepassingen die motorische, sensorische en/of cognitieve capaciteiten kunnen vergroten. Er zijn veel praktijkvoorbeelden bekend waarin werd gepoogd militaire prestaties te bevorderen met behulp van medicatie en stimulerende middelen.[26] Deze toepassingen waren vooral gericht op het bevorderen van fysieke gesteldheid.

Momenteel loopt er echter ook veel onderzoek naar het psychisch functioneren, en dan vooral hoe dit kan worden gemeten en beïnvloed.

22 R. Hoencamp, 'Afghanistan 2006-2010: medical aspects and challenges', in *Task Force Uruzgan* (2015).

23 Frederieke Jacobs, 'De medische voordelen van een virtuele wereld', SmartHealth 23 april 2015, http://www.smarthealth.nl/trendition/2015/04/23/de-medische-voordelen-van-een-virtuele-wereld/.

24 D. Coldewey, 'Duke neurosurgeons test Hololens as an AR assist on tricky procedures', 10 oktober 2016. Zie: https://techcrunch.com/2016/10/10/duke-neurosurgeons-test-hololens-as-an-ar-assist-on-tricky-procedures/.

25 D. Petruzello, 'Annual Report of Telemedicine & Advanced Technology Research Center', Frederick Maryland: United States Army Medical Research Center and Material Command (2009).

26 D. Shunk, 'Ethics and the Enhanced Soldier of the Near Future', Army Capabilities Integration Center, US Army januari-februari 2015, Zie: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20150228_art017.pdf.

FOTO MCD, E. VORSTENBOSCH

De traditionele, gevaarlijke manier van het afvoeren van gewonden. De Militaire Gezondheidszorg kijkt naar de mogelijkheden van autonome transportsystemen voor gewondenafvoer. Met behulp van een Unmanned Aerial Vehicle (UAV) zou men onafhandelijk van het terrein zijn

Binnen DARPA loopt het *silent talk* project, waarbij met behulp van *Brain-Computer-Interfaces* (BCIs) hersenactiviteit kan worden uitgelezen en worden vertaald in elektrische signalen.[27] Deze technologische ontwikkelingen gaan gepaard met manipulaties van het menselijk denken en handelen, en brengen dus risico's met zich mee en roepen ethische vragen op.
Voor de MGZ kunnen *human enhancement* toepassingen als preventieve maatregelen worden beschouwd die bijdragen aan duurzame inzetbaarheid van de individuele militair. Daarnaast kunnen de toepassingen zorgen voor verhoging van de individuele belastbaarheid en daarmee de operationele capaciteit vergroten.

Autonome MedEvac

Binnen de MGZ wordt er, net als in de civiele sector,[28] gekeken naar mogelijkheden van autonome transportsystemen. Er is behoefte aan autonome systemen voor gewondenafvoer vanwege het verhoogde risico voor de bestuurder tijdens een vuurgevecht. Een andere reden is de toenemende lengte van het voorterrein waarin een vuurgevecht plaatsvindt.[29]

27 Dr. G. Evans, 'Brain computer interfacing: a big step towards military mind-control', Army-Technology 17 juli 2013, http://www.army-technology.com/features/featurebrain-computer-interfacing-military-mind-control/. J.J. Shih, 'Brain-Computer Interfaces in Medicine', in *Mayo Clinic Proceedings* (2012) 87 (3) 268–279.

28 Ministerie van Infrastructuur en Milieu, 'Mobiliteit nu en in de toekomst', 28 oktober 2016, https://www.rijksoverheid.nl/onderwerpen/mobiliteit-nu-en-in-de-toekomst/inhoud/zelfrijdende-autos. J.M. Anderson, 'Autonomous Vehicle Technology', Santa Monica, California: RAND Corporation (2016).

29 E.D. Martin, 'Characteristics of the Future Battlefield and Deployment', in *Strategies to Protect the Health of Deployed U.S. Forces*, door National Research Council (US) Board on Environmental Studies and Toxicology, Washington (DC): National Academies Press (2000).

Met behulp van een *Unmanned Aerial Vehicle* (UAV) zou men echter onafhankelijk van het terrein zijn, en daardoor ook onder extreme omstandigheden kunnen voldoen aan de internationaal gehanteerde tijdslimieten.

Autonoom transport sluit het risico dat gepaard gaat met een vuurgevecht voor de gewonden helaas niet uit

In het kader van snellere, efficiëntere en veiligere MedEvac is de prioriteit van de ontwikkeling van autonome transportsystemen evident. Autonoom transport sluit het risico dat gepaard gaat met een vuurgevecht voor de te vervoeren gewonden echter niet uit. Er zijn namelijk ook ontwikkelingen waarbij UAV's door elektronische metingen op afstand kunnen worden uitgeschakeld.[30] Toch zijn er zowel internationaal – binnen krijgsmachten en het bedrijfsleven[31] – als nationaal al een aantal jaar hoopgevende ontwikkelingen gaande op dit gebied.[32]

Artificial Intelligence

Digitalisering, en dan met name ontwikkelingen op het gebied van *sensoring en monitoring*, gaat gepaard met het ontstaan van een grote hoeveelheid aan digitale data. Door de komst van internet kan deze data in zeer korte tijd voor zeer veel mensen toegankelijk worden gemaakt en wordt het genereren van nieuwe data gestimuleerd. Veel technologische ontwikkelingen dragen (in)direct bij aan de kwantiteit van digitale data, waardoor de hoeveelheid exponentieel toeneemt.

Sinds 2011 wordt te pas en te onpas de term *Big Data* gebruikt wanneer men spreekt over digitale data.[33] Men bedoelt dan meestal data van een grote hoeveelheid en een grote diversiteit, die met een hoge snelheid kan worden uitgewisseld. Er bestaat overigens geen eenduidige en algemeen geaccepteerde definitie van Big Data.[34] Big Data wordt bovendien echt relevant, wanneer er efficiënte methodes worden ontwikkeld waarmee relevante informatie uit deze grote hoeveelheid data gefilterd kan worden. Dit voedt de behoefte aan *Artifical Intelligence* (AI).

AI is moeilijk te bevatten en te omvatten, maar het is een domein waarover al sinds de Dartmouth Conferenties in 1956 met hoge verwachting wordt gesproken.[35] Er is geen eenduidige definitie van dit technologisch domein, maar volgens toonaangevende literatuur in dit vakgebied[36] zijn er vier verschillende benaderingen te onderscheiden: systemen die kunnen denken als mensen (ook wel *cognitive computing* genoemd);[37] systemen die kunnen handelen als mensen; systemen die rationeel kunnen denken; systemen die rationeel kunnen handelen. Men focust zich dus op het modelleren van menselijk functioneren, en dan vooral op het functioneren van het menselijk brein.

Met behulp van kleine processors, ook wel neuronen genoemd, kan een neuraal netwerk worden gecreëerd van verschillende lagen waarin willekeurige en onwillekeurige elektrisch signalen kunnen worden geïnitieerd en overgedragen.[38] Hierbij wordt het menselijk proces van leren gesimuleerd. Dit noemt men

30 D. Grossman, 'The Air Force Is Taking Down ISIS Drones Electronically', Popular Mechanics 24 oktober 2016, http://www.popularmechanics.com/military/weapons/a23525/usaf-attack-isis-drones-electronically/.

31 M. Cox, 'Firms Demonstrate Casualty Evacuation with Unmanned Helicopter', DefenseTech. 28 mei 2015, http://www.defensetech.org/2015/05/28/firms-demonstrate-casualty-evacuation-with-unmanned-helicopter/.

32 Webredaction communication TUDelft, 'Delftse 'dubbeldekkerdrone' delftAcopter vliegt met slechts een propeller', TU Delft 19 september 2016, http://www.tudelft.nl/nl/actueel/laatste-nieuws/artikel/detail/delftse-dubbeldekkerdrone-delftacopter-vliegt-met-slechts-een-propeller/.

33 J. Stuard Ward, 'Undefined By Data: A Survey of Big Data Definitions', arXiv Preprint (2013).

34 D. van Beek, 'Wat is Big Dat nu eigenlijk precies?' Dutch Bi Award, 11 juli 2015, https://www.biaward.nl/wat-is-big-data-nu-eigenlijk-precies/.

35 J. McCarthy, 'Proposal for the Dartmouth Summer Research Project on Artificial Intelligence', Hanover, New Hampshire: Dartmouth College (1955).

36 S. J. Russel, 'Artificial intelligence: A modern approach', Upper Saddle River: Prentice Hall (2003).

37 C. Rhinehart, 'The Impact of Cognitive Computing on Healthcare', International Business Machines Corporation, IBM Watson Health, 2015.

38 J. Schmidhuber, 'Deep learning in neural networks: An overview', in *Neural Networks* (2015) (61) 85-117.

ook wel *deep learning*. Het proces van deep learning wordt toegepast voor verschillende vormen van *machine learning*, onder meer in systemen voor spraak- en tekstherkenning.[39] Hierbij gaat het om een zelflerend systeem; een systeem dat getraind kan worden in het herkennen van patronen zonder vooraf vastgestelde voorwaarden en restricties.

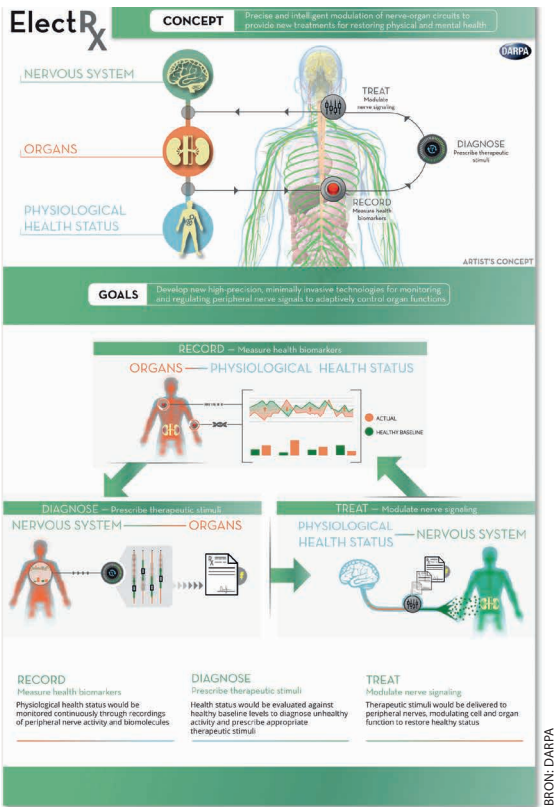
Momenteel zijn zowel marktleiders[40] als vele startups bezig met de ontwikkeling van AI voor het verwerken van onder meer medische Big Data.[41] Dit biedt potentiële kansen voor de MGZ om de kwaliteit en de efficiëntie van de zorg te stimuleren. Met behulp van deep learning en *data mining* kunnen structuren en verbanden worden bemerkt binnen ongestructureerde medische data, wat kan leiden tot nieuwe kennis en inzichten.[42] Dit kan bijdragen aan onder meer voorspellende geneeskunde, ziektepreventie en dus gezondheidsbevordering en inzicht in de inzetbaarheid.

Daarnaast wordt binnen de curatieve gezondheidszorg meer *symptom based medicine* mogelijk gemaakt, doordat een intelligent systeem, gebaseerd op Big Data, de meest waarschijnlijke diagnose kan stellen aan de hand van symptomen. De ontwikkeling van AI kan daarmee bijdragen aan optimalisatie van de MGZ in de vorm van meer *predictive, preventive and personalized medicine*.[43]

Ook in dit domein spelen ethische kwesties die relevant zijn voor Defensie. Grote spelers binnen dit domein benadrukken het risico van de mogelijkheid dat AI kan functioneren zonder menselijke invloed. Aangezien meerdere landen aan het experimenteren zijn met systemen die volledig autonoom kunnen opereren op basis van AI,[44] is het voor het kunnen beheersen van potentiële risico's essentieel om kennis en kunde beschikbaar te hebben.

Quantum computing

Men spreekt van digitale data wanneer de data een beperkt aantal discrete waarden kan aannemen in tegenstelling tot analoge data. Normaal gesproken is dit aantal discrete waarden beperkt tot twee en wordt er gesproken over een binaire waarde of variabele. Deze waarde, in de computerwereld 'bit' genoemd,



BRON: DARPA

Een schematische weergave van het intelligent monitoren van de zenuwbanen. Het doel ervan is nieuwe behandelingen te kunnen aanbieden die de fysieke en mentale gezondheid herstellen

39 M. Copeland, 'What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?', NVIDIA 29 juli 2016, https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/.

40 K. Finley, 'Tech Giants Team Up to Keep AI From Getting Out of Hand', Wired 28 september 2016, https://www.wired.com/2016/09/google-facebook-microsoft-tackle-ethics-ai/.

41 J. Jacobs, 'AI: terug van nooit weggeweest', SmartHealth 15 september 2016, http://www.smarthealth.nl/trendition/2016/09/15/kunstmatige-intelligentie-ai/.

42 Prasanna Desikan, 'Data Mining for Healthcare Management', SIAM International Conference on Data Mining, Mesa, Arizona USA: Society for Industrial and Applied Mathematics (2011).

43 L. Hood, 'Systems biology and new technologies enable predictive and preventative medicine', in *Science* (2004) 306(5696): 640-643. M. Swan, 'The Quantified: Fundamental Disruption in Big Data Science', in *Big Data* (2012) 1(2) 85-99. L. Ottes, 'Big Data in de Zorg', Working Paper 19, Wetenschappelijke Raad voor het Regeringsbeleid (2016).

44 S.J. Jr. Freedberg, 'Should US Unleash War Robots? Frank Kendall Vs. Bob Work, Army', Breaking Defense 16 augustus 2016, http://breakingdefense.com/2016/08/should-us-unleash-war-robots-frank-kendall-vs-bob-work-army/. TASS, 'Russia's remote-controlled Tigr armored vehicle shows fire power', Russian News Agency, 26 augustus 2016, http://tass.com/defense/896058.

wordt in veel gevallen aangeduid met 0 of 1 (aan of uit). Een quantum computer daarentegen maakt gebruik van quantum bits, of qubits, die een waarde kunnen hebben van 0, 1 of 0 en 1 tegelijkertijd. Hierdoor zijn deze computers in staat om met een grote hoeveelheid waardes tegelijk te rekenen.[45]

AI kan bijdragen aan optimalisatie van de MGZ in de vorm van meer voorspellende en gepersonaliseerde medicatie

Dit kan ook voor de medische wereld een belangrijke doorbraak betekenen. Met behulp van de rekenkracht van quantum computers kunnen complexe moleculaire interacties gemodelleerd en gesimuleerd worden, wat kan bijdragen aan de ontwikkeling van specifieke medicatie. Hierbij heerst de verwachting dat men met quantum computing binnen korte tijd in staat is om alle twintigduizend menselijke proteïnes te moduleren.[46]

Quantum computers op zich zullen niet direct een bijdrage leveren aan verhoging van de kwaliteit van de MGZ. De grote rekenkracht van quantum computers kan wel worden toegepast om de capaciteit van andere medische techniek te vergroten. Hierbij kan worden gedacht aan technologie waarbij medische data verwerkt dient te worden, zoals in toekomstige AI-systemen, of bijvoorbeeld veilige datauitwisseling tussen quantum computers met behulp van quantum teleportatie.[47] Quantum computing kan daarmee bijdragen aan een exponentiële ontwikkeling van technologieën die directe verbetering van de MGZ met zich mee kunnen brengen.

Blockchain technologie

Blockchain technologie is geen product maar een methode die kan bijdragen aan verhoging van efficiëntie en borging van kwaliteit.[48] Het is een digitaal grootboek waarin transacties worden gegenereerd en geregistreerd op alle computers die aangesloten zijn op het netwerk, oftewel de blockchain. Hiermee is het een gedecentraliseerd systeem zonder eigenaar, dat volledig transparant is voor elke schakel in het netwerk.

Voor het registreren van een transactie in het grootboek, moet de meerderheid van de computers uit de blockchain de transactie hebben geverifieerd aan de hand van cryptografische berekeningen.[49] Hiermee wordt voorkomen dat er ongewenste transacties worden gegenereerd of geregistreerd. Elke computer in het netwerk bevat namelijk een exacte kopie van het grootboek. Dus wanneer er getracht wordt een transactie te manipuleren, moet dit tegelijkertijd op alle aangesloten computers in het netwerk gebeuren, wat praktisch niet realiseerbaar is.[50]

Blockchain technologie kan mogelijkheden bieden voor de MGZ op het gebied van veilige en efficiënte datatransacties tussen het uitzendgebied en Nederland. Met behulp van de blockchain encryptie kan medische data worden uitgewisseld via internet, waarbij de betrouwbaarheid en kwaliteit van de brondata geborgd blijft. Doordat de berichten en transacties gedecentraliseerd worden opgeslagen, in plaats van op één locatie, is het systeem moeilijker te hacken en zou een eventuele poging ook sneller onderkend kunnen worden.

In plaats van een almaar toenemende afscherming van data ontstaat er door blockchain technologie meer zicht op wie de data bekijkt

45 A. Offerman, 'Kwantumcomputers komen eraan', Tweakers, 21 januari 2014, https://tweakers.net/reviews/3365/all/kwantumcomputers-razendsnel-rekenen-op-de-kleinste-deeltjes.html.

46 P. Diamandis, 'Massive Disruption Is Coming With Quantum Computing', SingularityHub 10 oktober 2016, http://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/.

47 G. van Hal, 'Quantumteleportatie verwijst bezwaren Einstein naar prullenbak', NewScientist 28 augustus 2015, https://newscientist.nl/nieuws/quantumteleportatie-verwijst-bezwaren-einstein-naar-prullenbak/.

48 R. van Zuidam,'Government-as-a-Service: Het nieuwe Nederlandse exportproduct', IntoBlockchain.com (2016).

49 L. de Vries, 'Waarom Blockchain een computerrevolutie is', AIR Café Blockchain, Stroe: AIR (2016).

50 D. Reijerman, 'De kracht van de blockchain - Innovaties met de ruggengraat van bitcoin', Tweakers 15 december 2014, https://tweakers.net/reviews/3781/all/de-kracht-van-de-blockchain.html.

en eventueel modificeert. Hiermee kan een snelle detectie van bedreigingen en behoud van integriteit van datasystemen plaatsvinden.[51] Zowel DARPA als de NAVO onderzoekt momenteel de militaire toepassingen van blockchain technologie.[52]

3D printen

3D printen biedt veel mogelijkheden om te voorzien in middelen wanneer er geen uitgebreide logistieke capaciteiten ter beschikking zijn. Dit lijkt voor Defensie een erg relevante technologie aangezien er steeds vaker kleinschalig wordt opgetreden. Bij aanwezigheid van 3D modellen en de benodigde grondstoffen kan er ter plekke specifieke productie plaatsvinden. Voor de operationele MGZ kan hierbij gedacht worden aan het 3D printen van voeding voor een specifiek dieet of bijvoorbeeld medicatie.[53] De operationele omstandigheden kunnen namelijk een specifieke behoefte aan voedingsstoffen en chemische stoffen teweeg brengen. Met behulp van 3D printen kan ter plekke worden ingespeeld op de zorgvraag van een individu, waardoor er preventieve en gepersonaliseerde gezondheidszorg kan plaatsvinden die bijdraagt aan de inzetbaarheid van de militair.

Voor de reguliere MGZ kan 3D printen een toegevoegde waarde hebben, zoals nu in civiele zorginstellingen ook al het geval is. Hierbij kan worden gedacht aan het 3D bioprinten van organen, ledematen of artificieel weefsel. De Amerikaanse krijgsmacht ziet veel potentie in deze toepassingen en investeert in het onderzoek en de ontwikkeling van 3D bioprinten van huidweefsel.[54] Hiermee zou verminking en beperking in beweging door verwondingen kunnen worden beperkt of verholpen. 3D printen heeft dus een militaire meerwaarde doordat het een bijdrage levert aan het behandelen en herstellen van militairen met gevechtsverwondingen.

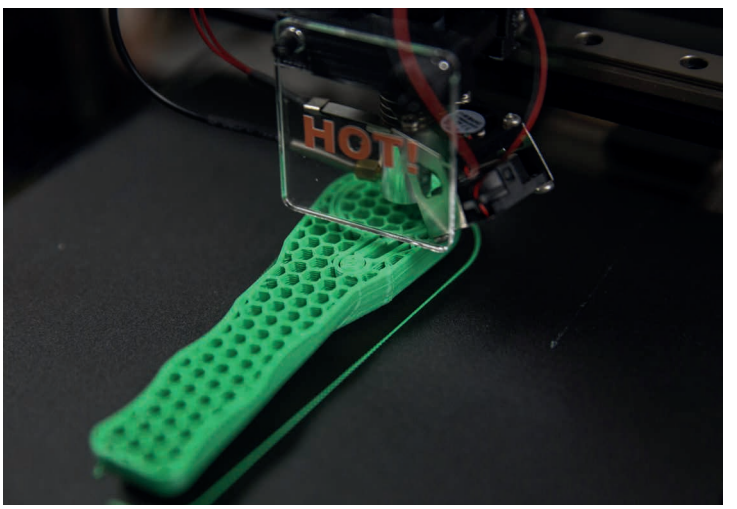


FOTO US MARINE CORPS, J. UPDEGRAFF

3D printen biedt veel mogelijkheden – van voeding tot het bioprinten van organen, ledematen of kunstmatig weefsel

Genomica & Biotechnologie

Genetische screening

Bij genetische screening of genetisch testen worden chromosomen, proteïnen en metabolieten van een specifiek gen geanalyseerd om bepaalde ziektebeelden te kunnen analyseren. Gnetische screening gaat om het routinematig testen op erfelijke afwijkingen in het DNA zonder dat er vooraf een verdenking is van een erfelijke afwijking. In 2008 waren er al 1200 genetische tests beschikbaar. Dit aantal stijgt jaarlijks met 25 procent.[55] Men probeert aan de hand van het DNA een verhoogd risico voor een bepaalde aandoening te achterhalen, zodat er eventueel maatregelen kunnen worden getroffen tegen de ontwikkeling van de ziekte.

Hierbij dienen *single nucleotide polymorphisms* (SNP's) als genetische merker.[56] De verwachting is dat de kosten van dergelijke DNA-technologieën binnen vijf jaar zullen afnemen met een factor duizend terwijl de beschikbaarheid zal toenemen.[57]

51 O. Ogundeji, 'US DARPA Takes Blockchain for Military Use', *Criptocoins News* 15 oktober 2016, https://www.cryptocoinsnews.com/us-darpa-takes-blockchain-for-military-use/.

52 G. Prisco, 'DARPA, NATO Looking at Military Applications of Blockchain Technology', Bitcoin Magazine 23 mei 2016, https://bitcoinmagazine.com/articles/darpa-nato-looking-at-military-applications-of-blockchain-technology-1464018766.

53 C. Lee Ventola, 'Medical Applications for 3D Printing: Current and Projected Uses', in *Pharmacy & Therapeutics* (2014) 39 (10) 704–711.

54 D. Lafontaine, 'Army invests in 3-D bioprinting to treat injured Soldiers', US Army 8 juli 2014, https://www.army.mil/article/129584.

55 D. Allingham-Hawkins, 'Successful Genetic Tests Are Predicated on Clinical Utility', in *Genetic Engineering & Biotechnology News* (2008) (28) no. 14.

56 A.C. Syvänen, 'Accessing genetic variation: genotyping single nucleotide polymorphisms', in *Nature Reviews Genetics* (2001) 930-942.

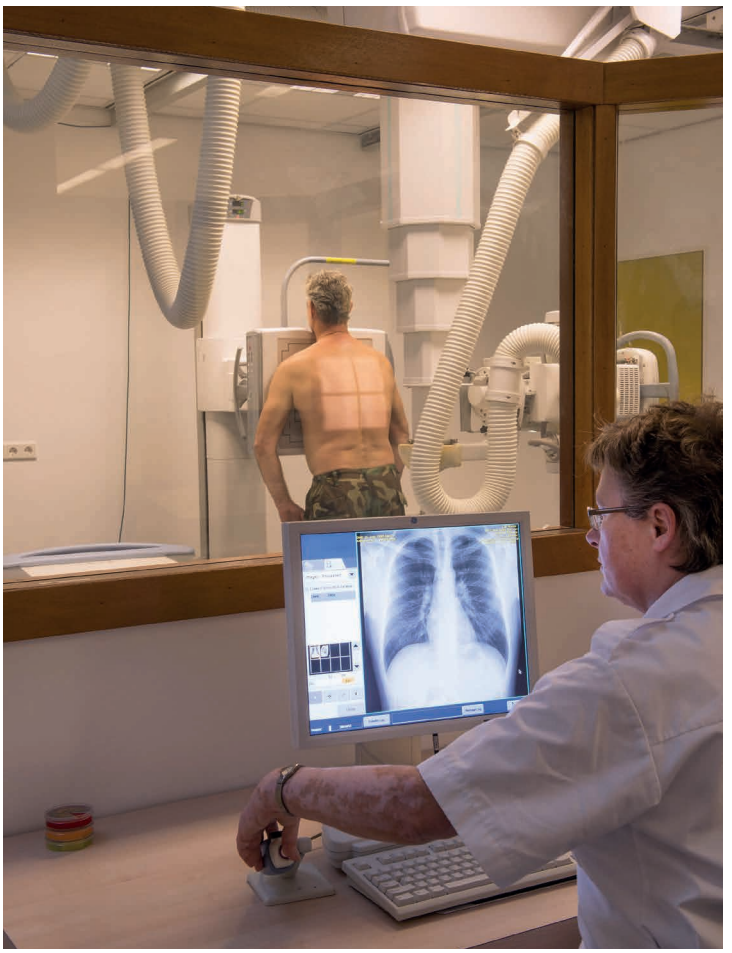


FOTO MCD, J. VAN HELVERT

Gezondheidszorg wordt steeds meer als een continuüm beschouwd van gezondheidsbevordering en ziektepreventie, waarbij de patiënt centraal staat

Voor Defensie biedt genetische analyse mogelijkheden om het genetisch profiel van elke militair in kaart te brengen. Hiermee kan men beter een inschatting maken van de fysieke en mentale kwaliteiten en kwetsbaarheden van een individu. Het genetisch profiel kan worden gekoppeld aan het persoonlijk medisch dossier, waardoor meer inzicht in de gezondheid en inzetbaarheid van dat individu ontstaat. Dit kan bijdragen aan preventieve maatregelen en gepersonaliseerde gezondheidszorg die is afgestemd op de operationele omstandigheden en de militaire taak.

Een militair met een mutatie in het RYR1 gen heeft bijvoorbeeld een verhoogde kans op warmte-gerelateerd letsel.[58] Met deze kennis kunnen voorzorgsmaatregelen worden getroffen voor missies bij hoge temperaturen, waardoor uitval van een individuele militair voorkomen kan worden. Bij implementatie van deze technologieën zal men echter het hoofd moeten bieden aan de uitdagingen die gepaard gaan met het gebruiken van persoonlijke gegevens. Dat dit niet eenvoudig is constateert ook de Amerikaanse krijgsmacht, die al jaren op zoek is naar mogelijkheden voor integer gebruik van genetisch data.[59] Daarnaast zal de ontwikkeling van deze technologieën nog een aantal stappen moeten maken voordat de toepassingen daadwerkelijk kostenefficiënt en dus relevant worden.

Genetische manipulatie

De grootste ontwikkeling op het gebied van genetische manipulatie vond begin 2013 plaats.[60] Dit was het moment waarop voor het eerst werd gepubliceerd over het CRISPR-Cas9 systeem.[61] Hiermee wordt men in staat gesteld om te 'knippen' op elke willekeurige plek in het menselijk genoom. Uiteindelijk kan hiermee, eventueel met behulp van externe factoren, de expressie van specifieke genen worden voorkomen of juist worden gestimuleerd. Deze ontwikkeling biedt tal van mogelijkheden voor het voorkomen of behandelen van ongewenste mutaties of expressies van het genoom, zoals bijvoorbeeld bij ziektes als kanker, alzheimer of Parkinson.

Het CRISPR-Cas 9 systeem is namelijk in staat om een zogeheten mutagene kettingreactie op gang te helpen.[62] Dat betekent voor geslachtscellen dat het gemuteerde gen automatisch

57 S. McShane, '3 DNA Technologies That Will Forever Change Your Home Life', SingularityHub 9 oktober 2016, http://singularityhub.com/2016/10/09/3-dna-technologies-that-will-forever-change-your-home-life/.

58 N. Dlamini, 'Mutations in RYR1 are a common cause of exertional myalgia and rhabdomyolysis', in Neuromuscul. Disord. (2013) 23, 540–548.

59 M. De Castro, 'Genomic Medicine in the Military', in *Npj Genomic Medicine* (2016) (1) no. 15008.

60 H. Ledford, 'CRISPR: gene editing is just the beginning', in *Nature* (2016) (531) 156–159.

61 CRISPR staat voor *Clustered Regularly Interspaced Short Palindromic Repeats*.

62 V. M. Gantz, 'The mutagenic chain reaction: A method for converting heterozygous to homozygous mutations', Science 19 maart 2015, http://science.sciencemag.org/content/early/2015/03/18/science.aaa5945.article-info.

wordt doorgegeven aan het nageslacht, en dat dit gen ook dominant zal zijn binnen elke nakomeling. Hierdoor volgt er een soort kettingreactie die lijkt op een virus dat zich uitspreidt over al het nageslacht.[63]

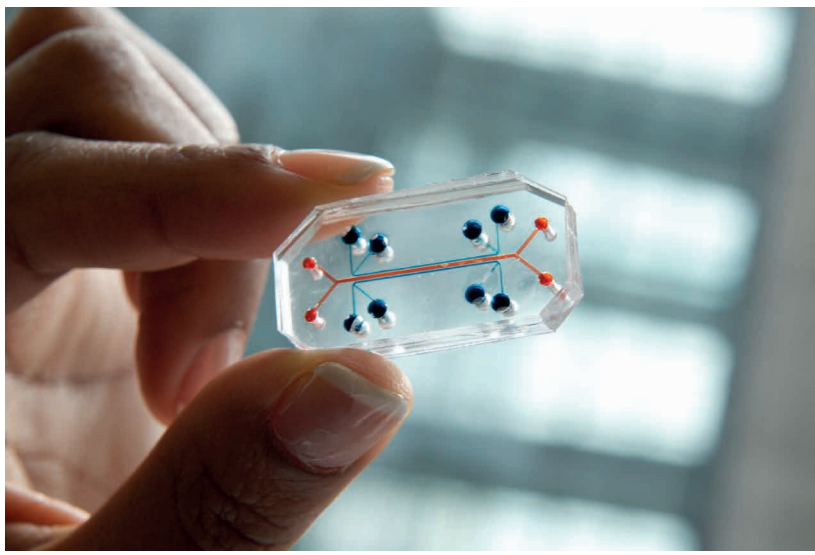
Met deze ontwikkeling lijkt de mogelijkheid te gaan ontstaan waarmee menselijk DNA naar eigen wens kan worden gemanipuleerd. Dit kan bijvoorbeeld ook worden toegepast voor het creëren van militairen die op basis van genetisch eigenschappen bestand zijn tegen extreme omstandigheden. Vergelijkbare experimenten vinden al plaats met dieren, zoals men in China honden kan creëren met extra spiermassa.[64]

Tegelijkertijd kunnen er door genetische manipulatie ongewenste mutaties optreden in het genoom, wat tot het ontstaan van nieuwe erfelijke aandoeningen kan leiden. Dit kan een grote uitwerking hebben op zorgprocessen en ziektebeelden binnen de gezondheidszorg. Hierbij is het overigens niet de vraag óf dit gaat gebeuren maar wanneer, en tot welke gevolgen dit gaat leiden. Er hebben namelijk al experimenten plaatsgevonden waarbij het genoom van gezonde menselijke embryo's is gemanipuleerd met de CRISPR-techniek.[65]

Deze ontwikkelingen kunnen van grote waarde zijn voor de geneeskunde, maar kunnen ook een bedreiging zijn voor de gezondheid van de mens. Het is daarom essentieel dat er zorgvuldig te werk wordt gegaan. Daarbij is adequaat toezicht en wet- en regelgeving cruciaal. Het Amerikaanse DARPA heeft om die reden een programma heeft opgezet om de ontwikkelingen op het gebied van genetische manipulatie te kunnen beheersen.[66] Ook voor de MGZ is het relevant om te beseffen hoe deze techniek zich ontwikkelt.

Nanomedicine

Dit vakgebied houdt zich bezig met het ontwikkelen van medische toepassingen op een schaal van nanometers met een functie op cellulair, moleculair of anatomisch niveau.[67] Hierbij zoekt men naar geschikte eigenschappen van elementaire materialen of stoffen die



BRON: DARPA

Het gebruik van nanotechnologie, zoals deze artificiële long gemodelleerd op een chip, heeft binnen de gezondheidszorg op veel gebieden een potentiële meerwaarde

gebruikt kunnen worden voor toepassingen op zeer kleine schaal. Doordat men bij veel toepassingen van nanotechnologie gebruik maakt van de eigenschappen van de stof zelf, wordt het functioneren niet beïnvloed door de grootte van het materiaal.

Binnen de gezondheidszorg zijn er veel toepassingen waarin het gebruik van nanotechnologie een potentiële meerwaarde vormt. Bijvoorbeeld binnen het domein van *nano drug delivery*,[68] waarbij medicamenten binden op een specifieke plaats in het menselijk lichaam die behandeling behoeft. Dit maakt het mogelijk dat het omliggende weefsel gespaard blijft en het *target*

63 A. Jaspers, 'Doorbraak van het jaar: CRISPR - Hoop en vrees over 'genetische kettingreactie'', De Kennis Van Nu, 21 december 2015, http://www.dekennisvannu.nl/site/artikel/Doorbraak-van-het-jaar-CRISPR---Hoop-en-vrees-over-genetische-kettingreactie/7111.

64 C. Larson, 'China's Bold Push into Genetically Customized Animals', Scientific American 17 november 2015, https://www.scientificamerican.com/article/china-s-bold-push-into-genetically-customized-animals/.

65 R. Stein, 'Breaking Taboo, Swedish Scientist Seeks To Edit DNA Of Healthy Human Embryos', 22 september 2016, http://linkis.com/www.npr.org/sections/kkLeM.

66 DARPA, 'Setting a Safe Course for Gene Editing Research', Defence Advanced Research Projects Agency 7 september 2016, http://www.darpa.mil/news-events/2016-09-07.

67 S. Sandhiya, 'Emerging trends of nanomedicine–an overview', in *Fundamental & Clinical Pharmacology* (2009) 23 (3) 263-9.

68 J. Safari, 'Advanced drug delivery systems: Nanotechnology of health design A review', in *Journal of Saudi Chemical Society* (2014) 85-99.

FOTO MCD, B. NIJS

De meestvoorkomende oorzaak van sterfgevallen tijdens missies (66 procent) is het niet tijdig kunnen stoppen van een bloeding. Nanobots die bloedstolling stimuleren lijken dan ook een zeer relevante toepassing van nanotechnologie voor Defensie

weefsel juist van een hogere dosering voorzien kan worden. Men is vooral bezig met deze methode toe te passen voor de behandeling van kanker. Nanodeeltjes of nanobots hebben namelijk bij verschillende ziektes meerdere voordelen ten opzichte van lichaamseigen cellen van het immuunsysteem.[69]

Binnen de nanotechnologie is er ook een ontwikkeling gaande die voor de MGZ zeer relevante is. Nanobots kunnen namelijk worden ingezet om bloedingen in zeer korte tijd te stoppen. Deze zeer kleine kunstmatige mechanische bloedplaatjes bevorderen het functioneren van stollingslichaampjes en verhogen de concentratie op de plek van de bloeding, om bloedverlies te beperken.[70]

69 M. Saha, 'Nanomedicine: Promising Tiny Machine for the Healthcare in Future-A Review', in *Oman Medical Journal* (2009) 24 (4) 242–247.

70 F. Alam, 'Nanotechnology-based artificial platelets', in *Egyptian Journal of Haematology* (2014) 39 (1)1-5.

71 A.N. Ilinskaya, *'Nanoparticles and the blood coagulation system. Part I: benefits of nanotechnology', in* Nanomedicine (2013) 8 (5) 773-784.

Hierbij zijn er type nanodeeltjes die de bloedstolling bevorderen, maar ook type nanodeeltjes die bloedstolling kunnen belemmeren of vertragen.[71]

De voordelen van het gebruik van nanodeeltjes in het bloedstollingsmechanisme zijn dat de dosis verlaagd kan worden, er doelgerichter kan worden afgegeven, en een afweerreactie overwonnen kan worden. Deze toepassingen kunnen een belangrijke rol kunnen spelen in het stoppen van bloedingen bij gewonde militairen. Hiermee zou het aantal sterfgevallen tijdens missies mogelijk geminimaliseerd kunnen worden. De meest voorkomende oorzaak van sterfgevallen tijdens missies is namelijk het niet tijdig kunnen stoppen van een bloeding. Uit onderzoek[72] blijkt dat 66 procent van de gewonden bij een vuurgevecht binnen tien minuten sterft, van wie de helft sterft aan bloedingen. Nanobots die bloedstolling stimuleren lijken dan ook een zeer relevante toepassing van nanotechnologie voor Defensie.

Kortom

In dit artikel kwamen medisch technologische ontwikkelingen aan de orde die binnen Defensie een bijdrage kunnen leveren aan zowel genezing van ziekte als bevordering van de gezondheid. Als we kijken naar de toepassingen in de categorie Sensoring & Monitoring is de conclusie dat het gaat om concrete producten, die civiel gerealiseerd en geïmplementeerd zijn. Voor Defensie liggen hier dus kansen die direct benut kunnen worden.

De categorie Robotica & AI beschrijft daarentegen concepten, waarvan het gebruik momenteel voornamelijk beperkt wordt tot *early adopters*. Maar dit zijn wel ontwikkelingen die een ingrijpend effect kunnen hebben op de bevordering van kwaliteit en die een efficiëntere werkwijze teweeg kunnen brengen binnen de MGZ. Defensie zou daarom de samenwerking kunnen aangaan met externe partijen, met name onderzoeksinstituten, om de ontwikkeling van deze concepten voor militaire toepassing te stimuleren.

Wat betreft de categorie Genomica & Biotechnologie is het voor Defensie relevant om te beseffen welke potentiële risico's er gepaard gaan met deze ontwikkelingen. Eventueel in samenwerking met externe partijen dienen ontwikkelingen gemonitord te worden om te kunnen participeren in beheersmaatregelen.

De toegevoegde waarde van technologische toepassingen wordt niet alleen bepaald door de techniek op zich. Optimale randvoorwaarden zijn nodig, zowel op het gebied van mensen als middelen

Toepassingen van Nanotechnologie zitten voornamelijk nog in onderzoeks- en ontwikkelingsfase. Voor Defensie lijkt het niet relevant om voorloper te zijn binnen dit vakgebied, maar ze kan wel profiteren van toepassingen die civiel worden ontwikkeld en beproefd.

Zoals eerder gesteld, zijn de omschrijvingen van de potentiële relevante technologische ontwikkelingen niet allesomvattend. Daarnaast dient men zich te realiseren dat de toegevoegde waarde van technologische toepassingen niet alleen bepaald wordt door de techniek op zich. Efficiënte implementatie van medische techniek vergt optimale randvoorwaarden, zowel op het gebied van mensen als middelen. Het is dan ook voor Defensie belangrijk om te investeren in personele capaciteit die de implementatie en het gebruik van innovatieve medische techniek bevordert. Dat optimaliseert de kwaliteit van de geleverde zorg en draagt zo bij aan een organisatie die het vermogen heeft om flexibel en adaptief te zijn in een veranderende wereld. ■

72 R. Hoencamp, 'Afghanistan 2006-2010: medical aspects and challenges', in: *Task Force Uruzgan* (2015).

In deze *Militaire Spectator* is plaatsgemaakt voor een gastcolumn. W.M. Oppedijk van Veen schrijft over veiligheidsrisico's in relatie tot de Nederlandse defensiebegroting. 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) of aanbieden via de website. De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur

Defensiebegroting: waar is de urgentie en het *commitment*?

*Prof. dr. W.M. Oppedijk van Veen**

In *NRC Handelsblad* van 20 januari 2017 schetst de vermaarde publicist en hooggeleerde historicus Ian Buruma een nogal somber toekomstperspectief. Gebrek aan Amerikaans leiderschap en een militair verzwakt Europa leiden er toe dat landen als China en Rusland in toenemende mate het Westen uitdagen en de grenzen van hun macht zullen opzoeken. Er hoeft maar iets fout te gaan – een uit de hand gelopen grensconflict, een neergeschoten vliegtuig, een vermiste onderzeeboot of een bom op een stad – en we worden ongewild en tegen elk gezond verstand een oorlog ingerommeld.

Bij herhaling laat de minister van Defensie blijken dat ze de veiligheidsrisico's van het Russische optreden in bijvoorbeeld de Baltische staten, Oekraïne en de Krim onderkent, maar ook dat de Nederlandse strijdkrachten niet meer in staat zijn de essentiële belangen van Nederland en het Nederlandse grondgebied te verdedigen. Desondanks memoreerde de minister met enige trots dat de strijdkrachten in de afgelopen vier jaar bijna 900 miljoen extra hebben gekregen.[1] Dat is nog geen 250 miljoen op jaarbasis: net genoeg om de ergste nood te lenigen en om eerder geplande bezuinigingen een halt toe te roepen. Onvoldoende inzetbaar materieel en geoefend personeel blijft voorlopig echter de realiteit.

De veiligheidsrisico's zijn misschien op zich nog niet zo groot, maar ze worden aanzienlijk groter wanneer twijfel gaat bestaan over de bereidheid van Amerika zijn Europese bondgenoten te hulp te komen. Van enige urgentie is nu nog niet veel te merken. Volgens de minister gaat het nog vele jaren duren voordat de krijgsmacht weer op orde is en de weg daar naar toe zal slechts met kleine stapjes zijn. Daarbij, het scenario waarbij Nederlands grondgebied direct betrokken raakt bij een klassieke aanval wordt niet erg waarschijnlijk geacht.[2] Maar in combinatie met een vergaande cyberaanval zouden de gevolgen voor Nederland wel eens dramatisch kunnen zijn als het daadwerkelijk een keer fout gaat.[3] Mij zijn hiervan geen officiële scenario's bekend, maar duizenden slachtoffers en totale ontwrichting van de samenleving en economie als gevolg van

* Met dank aan luitenant-generaal b.d. J.A. van Diepenbrugge en reserve ritmeester b.d. mr. P. van den Brandhof voor hun kritische commentaar.

1 *Buitenhof*, zondag 21 januari 2017.

2 *Veilige Wereld, Veilig Nederland: Internationale veiligheidsstrategie* (https://www.rijksoverheid.nl/documenten/rapporten/2013/06/21/veilige-wereld-veilig-nederland-internationale-veiligheidsstrategie).

3 Het is altijd die ene keer, dat het meest onwaarschijnlijke toch werkelijkheid wordt, die telt. Zie N.M. Taleb, *The Black Swan. The Impact of the Highly Improbable* (Londen, Penguin Books, 2008).

grootschalige lamlegging of vernietiging van infrastructuur en productiecapaciteiten ligt in de rede. Om in een dergelijke situatie voornamelijk te moeten vertrouwen op de militaire inzet van bondgenoten gaat voorbij aan de grondwettelijke taak van Nederland – dat daarin zelf een primaire verantwoordelijkheid heeft – en getuigt van een overwaardering van de bereidheid, de beschikbaarheid en de gelegenheid van de bondgenoten om in een chaotische en actuele oorlogssituatie Nederland daadwerkelijk militair bij te staan.

Volgens de afspraken binnen het NAVO-bondgenootschap moeten de deelnemende landen – en dus ook Nederland – minimaal twee procent van het bruto binnenlands product (bbp) besteden aan defensie. Op basis van de cijfers van 2017 zou dat neerkomen op circa 14 miljard euro, wat ongeveer een verdubbeling van het budget is dat Defensie nu beschikbaar heeft voor typisch militaire taken.[4] Met uitzondering van het Verenigd Koninkrijk, Estland Polen en Griekenland lijkt echter geen van de overige 22 Europese NAVO-landen een dergelijk niveau van defensie-uitgaven te gaan realiseren; gemiddeld blijven ze steken op 1,43 procent van het bbp. Onze minister noemde in haar *Buitenhof*-interview die twee procent dan ook slechts een streefpercentage en stelde dat de versterking van de krijgsmacht vooral gevonden moet worden in de samenwerking met onze NAVO-bondgenoten die ook te weinig besteden. En inderdaad, die samenwerking verloopt nu eenmaal niet gemakkelijk en vergt aanvankelijk zelfs nieuwe investeringen. Ook de vereiste instemming van de betrokken nationale parlementen bij een daadwerkelijke inzet van internationaal georganiseerde militaire capaciteiten is niet bevorderlijk voor een vergaande militaire samenwerking. Dus de twee procent en ook het gemiddelde NAVO-bestedingsniveau van 1,43 procent zal in Nederland bij lange na niet op korte termijn gehaald worden.

De centrale vraag is dan ook wat die NAVO-afspraken, recentelijk herbevestigd in Warschau, waard zijn en waar de urgentie en het *commitment* is om ten minste het gemiddelde bestedingsniveau van 1,43 procent van het bbp als een eerste afspraak te zien die op afzienbare termijn moet worden nagekomen en waarop bewindslieden en bestuurders kunnen worden afgerekend.

Sinds het aftreden van generaal Van der Vlis, meer dan twintig jaar geleden, die zich niet kon vinden in de eerste grote bezuinigingen, is er geen minister, hoge ambtenaar of generaal (Commandant der Strijdkrachten of Commandant Operationeel Commando) geweest die de afgelopen jaren zijn functie ter beschikking heeft gesteld omdat hij zich niet kon vinden in de omvang en aard van de defensiebesparingen. Ongetwijfeld zullen nobele motieven een rol hebben gespeeld: ‘om het beste er van te maken moet je er wel bij zijn’ en ‘als de politiek bepaalt, dan heb je maar te volgen’. Maar dat op dit moment binnen de krijgsmacht twee derde van het personeel geen vertrouwen heeft in de (militaire, ambtelijke en politieke) top van de defensieorganisatie, kan niet anders opgevat worden dan als een enorme diskwalificatie van die top en dient hen zwaar aangerekend te worden.[5]

Misschien dat het nu tijd is voor een wat steviger houding. Het wordt er intussen immers niet veiliger op. En, zoals K.J.L Walenkamp in de *Militaire Spectator* van januari 2017 zo helder schetste, de tijd lijkt voorbij dat Defensie gezien werd als slechts een kostenpost en als een weinig belangrijk beleidsdomein.[6] Tijd om door te pakken dus! ■

4 De defensiebegroting 2017 van circa 8,7 miljard euro bestaat voor ongeveer een kwart tot een derde uit middelen bestemd voor oude en lopende pensioenverplichtingen en taken ter ondersteuning van de civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp.

5 Zie: http://www.eenvandaag.nl/uploads/doc/Enquete_personeel2016-definitief.pdf.

6 K.J.L. Walenkamp, ‘Een strijd om de defensiebegroting’, in: *Militaire Spectator* 186 (2017) (1) 4-18.

Open brief aan ons nieuwe parlement

Oorlog is in Europa de voortzetting van politiek, maar dan zonder middelen...[1]

*Frans Matser – publicist**

De komende jaren zal het economische en politieke krachtenspel in de wereld flink veranderen. De afgelopen 70 jaar kenmerkt de Europese geschiedenis zich door de afwezigheid van oorlog en een gestaag toenemende welvaart. Deze ontwikkeling beperkte zich *grosso modo* tot de westerse wereld. De gemiddelde Nederlander heeft het tegenwoordig beter dan de generaties voor ons. We hebben een huis, een auto, een televisie, een computer en gaan minstens één keer per jaar op vakantie. Als we ziek zijn staat een prima gezondheidssysteem voor ons klaar. We hebben uitstekend en betaalbaar onderwijs, persvrijheid en een uitgebreid systeem van regels en wetten dat onze rechten waarborgt, ook als je homoseksueel of allochtoon bent. Inmiddels zijn wij aan onze welvaart gewend. Je kunt zelfs zeggen dat we er aan zijn verslaafd! Als je Nederlanders vraagt wat 'eerste levensbehoeften' zijn, dan zijn velen van mening dat 25 vakantiedagen, een 36-urige werkweek, een computer, een smartphone, een auto en betaalbare gezondheidszorg daar absoluut bijhoren. De realiteit is dat 90 procent van de wereldbevolking die dingen niet heeft.

De mondiale schaduwzijde van onze welvaart is dat al deze voorrechten in de afgelopen honderd jaar voorbehouden zijn gebleven aan slechts 10 procent van de wereldbevolking; zo'n 600 miljoen mensen. Grote delen van de bevolking van Azië, Oost-Europa, Afrika en Zuid-Amerika leefden in de 20ste eeuw in armoede, werden onderdrukt en met regelmaat geteisterd door hongersnoden, onderdrukking door megalomane dictators, religieus geweld, natuurrampen en oorlogen. Nog steeds hebben miljarden wereldburgers nauwelijks toegang tot goede opleidingen, gelijke rechten of goede medische voorzieningen.

Onze welvaart staat momenteel onder druk. We zijn de afgelopen jaren getroffen door de bankencrisis, de huizen-crisis, de euro-crisis, en de vluchtelingen-crisis. Daardoor zijn we als land met z'n allen gewoon minder gaan verdienen. Grote delen van de wereldproductie aan goederen en diensten verplaatsten zich naar nieuwe opkomende economieën. Het lijkt dat de eenzijdige economische dominantie van de westerse wereld tanende is. Ook honderden miljoenen Chinezen, Indiërs, Mexicanen, Polen, Turken of Brazilianen willen een baan, een huis, een autootje, een televisietoestel en af en toe een stukje vlees op tafel. En wie geeft ze ongelijk! Overigens is het in deze landen vanzelfsprekend dat toenemende welvaart voor een deel geïnvesteerd wordt in hun krijgsmacht. Een krijgsmacht die er is om de belangen van het land te dienen.

Er zal dus de komende jaren, naast een ideologisch strijd tegen het terrorisme, ook een economisch 'strijd' ontbranden tussen de 600 miljoen mensen in de 'oude' welvarende wereld en de miljarden mensen in de 'opkomende' economieën. Daarbij hebben de nieuwelingen op termijn de betere papieren. Daar zijn ze nog *mean* en *lean*, en wij zijn behoorlijk soft en kwetsbaar geworden achter de brede rug van de

* Op deze plaats vindt u afwisselend een bijdrage van Frans Matser, publicist, en dr. M.F.J. Houben, luitenant-kolonel der mariniers.

1. Vrij naar Clausewitz.

Amerikanen. Of wij daarbij 10, 20 of 30 procent van onze welvaart inleveren, valt nog te bezien.

De vluchtelingenstromen worden nu (tijdelijk) voor ons gestopt door ons bevriende staatshoofd Erdogan, maar tegen welke prijs? Omdat de Turken en andere opkomende economieën vinden dat ze daar recht op hebben. Omdat ze het welvarende, betweterige Europa met het opgeheven (mensenrechten)vingertje zat zijn. Om hun streven te ondersteunen zullen ze zo nodig ook militaire middelen gebruiken. Als twee partijen even sterk zijn, is oorlog doorgaans geen optie. Het risico is te groot. Denk aan de situatie tussen NAVO en Warschaupact van 1950 tot 1990. Beide partijen probeerden op economische en politieke manier de bovenhand te krijgen, maar geen van beide greep naar de wapens. Het blijft daarom essentieel dat we in Europa voldoende militair vermogen overhouden, of we dat leuk vinden of niet. Als we de huidige situatie goed bekijken, dan zien we dat alle Europese landen hun krijgsmachten in de afgelopen twintig jaar tot het bot hebben afgebroken. Europa kan zichzelf al lang niet meer verdedigen en speelt militair nauwelijks meer een rol op het wereldtoneel. Met Trump aan de macht in de VS, is het ineens niet meer zo zeker dat de Amerikanen voor ons de kastanjes uit het vuur halen. Dit is een historische breuk met het verleden, maar ook een *wake-up call*. De rijkste landen van de wereld hebben de zwakste defensie! Dat geldt ook voor Nederland. Terwijl in landen als China, Rusland, Turkije en India in de afgelopen jaren het ene na het andere oorlogsschip van de helling rolde, rolde in Europa en dus ook Nederland het ene na het andere bezuinigingsplan uit de koker van de beleidsmakers.

Het Chinese defensiebudget groeit al twintig jaar met jaarlijks zo'n tien procent of meer. Op dit moment is China bezig grote delen van Afrika onder zijn invloedsfeer te brengen. Ook de Russen hebben de afgelopen tien jaar veel geld in de modernisering van hun krijgsmacht geïnvesteerd en zijn bezig aan een offensief om hun invloedssferen te herstellen. India en Indonesië zijn Azië aan het verdelen. En in Noord-Afrika gist het gif van het religieuze fundamentalisme, waarbij NAVO-partner Turkije een tweeslachtige rol speelt. Dit zijn allemaal gebieden die tot voor kort onze economische achtertuin waren; waar wij grondstoffen, halffabricaten en goedkope arbeidskrachten weghaalden. Wie niet inziet dat dit op termijn spanningen gaat opleveren, heeft geen lessen geleerd uit de geschiedenis van de afgelopen honderd jaar. De afwezigheid van oorlog in Europa gedurende 70 jaar, onder de bescherming van de VS, heeft velen van ons doen vergeten dat het uiteindelijk militaire middelen waren die in 1945 vrede en vrijheid naar ons land hebben gebracht, niet mooie praatjes. Wie, zoals Nederland, slechts 1 procent van zijn welvaart aan defensie wil spenderen, krijgt daar op enig moment de rekening voor gepresenteerd.

Naïeve geesten in Nederland denken al jaren dat de wereldvrede is uitgebroken. Maar als de opkomende economieën hun deel van de koek komen opeisen, zullen ze gebruikmaken van politieke, economische én waar nodig ook militaire middelen. En als wij niet zorgen dat we tegenspel kunnen bieden op elk van die drie terreinen, dan zullen we kissebissend over euro, BREXIT en open grenzen in Europa de slag om onze welvaart en onze vrijheid verliezen. De bezuinigingen op de Europese en zeker de Nederlandse strijdkrachten van de afgelopen jaren zijn in dat licht stappen op de weg naar het verkwanselen van onze welvaart en onze vrije samenleving.

Dat we als Nederlanders op termijn moeten inleveren, is voor iedereen die het voorgaande verhaal heeft begrepen duidelijk. De koek is niet oneindig en zal onvermijdelijk 'anders' over de wereld verdeeld worden. De mate waarin we een deel van onze welvaart en vrijheid kunnen vasthouden, is mede afhankelijk van de mate waarin we in Europa in staat zullen zijn om ook militair ons mannetje te staan. Daarom moeten we ook in Nederland Defensie niet langer zien als een vervelende kostenpost, maar als een absoluut noodzakelijke verzekering. Onze krijgsmacht moet namelijk primair aan anderen duidelijk maken dat we bereid zijn om onze vrijheid en onze welvaart te verdedigen: figuurlijk, maar zo nodig ook letterlijk. Want wie vrede en vrijheid liefheeft, dient zijn krijgsmacht te koesteren. ■

Geld gooien

Linda Polman

Op 25 maart 2015 begon Saoedi-Arabië zijn oorlog tegen opstandelingen in Jemen. Die dag verscheen op de site van het Witte Huis de mededeling dat Amerika logistieke steun ging verlenen aan die strijd.
Aan generaal Lloyd J. Austin, toen bevelvoerder van het U.S. Central Command, werd de volgende ochtend gevraagd wat het militaire doel van de Amerikaanse steun was en hoe hij dacht dat doel te gaan bereiken. 'Ik weet niet wat het doel is,' antwoordde hij. 'Om te weten hoe waarschijnlijk het is dat we het doel gaan bereiken, zou ik dat eerst moeten weten.' De een zegt dat Iran het doel was: Iran zou de Jemenitische rebellen steunen en president Obama wilde de regio laten zien dat hij bereid was om tegen Iran op te treden. De ander zegt dat Obama niet veel keuze had: als hij niet voor Saoedi-Arabië zou hebben gekozen, hadden de Russen of de Chinezen dat wel gedaan. Misschien waren het wel de 60 miljard dollar aan *state-of-the-art* bommen, raketten en vliegtuigen die Amerika sinds 2010 aan Saoedi-Arabië had verkocht. Obama wist dat er méér was waar dat geld vandaan kwam.
Wat Saoedi-Arabië met al die dure spullen precies dacht te bereiken was ook niet helder. We zijn ruim twee jaar verder. Irans invloed in het Midden-Oosten is alleen maar gegroeid en de rebellen, velen op teenslippers en met een ouwe Kalasjnikov, hebben zich nog steeds niet overgegeven. Saoedi-Arabië maakt er in Jemen een potje van, zeggen waarnemers. Bij hun bombardementen met de dure Amerikaanse jets kwamen al meer dan 5000 burgers om het leven, een veelvoud daarvan raakte gewond. De Amerikanen zijn inmiddels maar aangeschoven bij het commando in Riyadh om de Saoedi's te helpen bij het nauwkeuriger bepalen van de coördinaten van hun aanvalsdoelen. Na een bommenregen op een markt waarbij tenminste 97 burgers om het leven kwamen, leende Amerika uit eigen voorraad precisie-bommen uit aan de Saoedi's, die moeten helpen bij beter mikken. Het kost tijd voordat een land om kan gaan met gevanceerde wapensystemen, zei een gegeneerde Matthew Spence, onder Obama de Deputy Assistant Secretary of Defense voor het Midden-Oosten. 'Maar stapje voor stapje zullen ze het leren.' Niet dat Saoedi-Arabië's hart bloedt voor burgerslachtoffers. Saoedi-Arabië gooit gewoon overal oliedollars tegenaan, dan verdwijnen problemen vanzelf. In 2016 bijvoorbeeld presenteerde de VN-Veiligheidsraad zijn jaarlijkse rapport over krijgsmachten die het oorlogsrecht schenden. Saoedi-Arabie overtrad dat jaar 152 keer de internationale verdragen met bombardementen op scholen, woonwijken, ziekenhuizen en markten. Het rapport was nauwelijks verschenen, of het verdween alweer, en verscheen toen opnieuw, maar zónder Saoedi-Arabië erin. De VN-secretaris-generaal, toen nog Ban Ki-moon, kwam er rond voor uit: Saoedi-Arabië had de VN bedreigd. Ze zouden de geldkraan dichtdraaien voor humanitaire VN-operaties in Zuid-Sudan en Syrië, als de naam Saoedi-Arabië niet uit het rapport verwijderd zou worden.
Niemand ook die durft in te grijpen nu de olieziljonairs de Jemenetische rebellen opzettelijk aan het uithongeren zijn. Een zeeblokkade door schepen van Saoedi-Arabië en een paar bondgenoten zorgt ervoor dat er geen voedsel en medicijnen het land meer binnenkomen. De hongersnood die het gevolg is heeft Saoedi-Arabië simpelweg opgekocht. Als volgt: de Saoedi's maakten van zichzelf de grootste hulpdonor aan Jemen. Andere donoren staan niet te trappelen om Jemen te hulp te komen, dus de VN heeft geen keuze dan dankuwel tegen de Saoedische donaties te zeggen. De hulpdollars zijn echter aan strenge voorwaarden gebonden. De humanitaire VN-organisaties mogen de hulpfondsen uitsluitend besteden waar en aan wie de Saoedi's het goed vinden. Dat is dus *niet* in rebellengebied en *niet* aan bevolkingsgroepen die de Saoedi's niet gunstig gezind zijn.
Zo bepaalt in Jemen de partij die de hongersnood veroorzaakt, wie VN-voedselhulp krijgt en wie niet. In april dit jaar zamelde Giro 555 geld in om honger te bestrijden, onder meer in Jemen. Ik voorspel dat die hongersnood er gewoon toch komt, maar precies op die plekken waar Saoedi-Arabië het graag ziet. ■

Lobbyland

De geheime krachten in Den Haag
Door Ariejan Korteweg en Eline Huisman
Amsterdam (De Geus) 2016
256 blz.
ISBN 9789044538106
€ 19,99

Lobbyen is onontbeerlijk in een democratie en zeker in polderend Nederland. Lobbyen gaat over het beïnvloeden van besluitvorming, waarbij allerhande belangengroepen invloed proberen uit te oefenen op politieke processen. Dit is belangrijk in een democratisch bestuur waarin burgers actief participeren. Lobbyen heeft ook een negatieve bijklank, namelijk manipulatie. De gerenommeerde onderzoeksjournalisten Ariejan Korteweg en Eline Huisman gaan in *Lobbyland* op zoek naar de stand van het lobbyen in de Nederlandse politiek en in het bestuur. In hun zoektocht benaderen ze lobbyen vanuit twee perspectieven: als noodzakelijke smeerolie in de Haagse poldermachine en als het ultieme middel om het Binnenhof als gesloten circuit in stand te houden.

Soorten lobbyisten

Lobbyen verwijst naar de *lobbies*, de wandelgangen van het Britse Lagerhuis waar belangenbehartigers de passerende parlementsleden nog gauw even konden aanschieten voor een informeel overleg. Lobbyisten zijn er in drie soorten: beroepslobbyisten, *practitioners* van PR-bedrijven en incidentele of gelegenheidslobbyisten. Het zijn belangenbehartigers die niet graag als lobbyisten worden herkend; bescheidenheid en discretie horen logischerwijze bij de etiquette van het vak. Een gouden regel is 'hoe geruislozer, hoe beter'. Beïnvloeding staat aan het fundament van lobbyen. Dit duidt ook de complexiteit van de zoektocht van Korteweg en Huisman: 'Beïnvloeding draait om sociale interacties. Die kun je nu eenmaal niet tot op de draad ontrafelen.' Bovendien, in de tegenwoordige Nederlandse context is lobbyen overal, bijvoorbeeld 'in Luden, de Haagse Kluis, Plein XIX, Schlemmer, De Posthoorn en al die andere cafés aan en om het Plein.' De auteurs doen echter een geslaagde poging. *Lobbyland* schetst een intrigerend beeld hoe politieke beïnvloeding in Nederland werkt. Lobbyen is noodzakelijk en maatwerk, maar het is ook beladen. Het maakt de zoektocht naar de stand van zaken in lobbyend Nederland des te interessanter.

Samenbrengen, verbinden, bemiddelen

Korteweg en Huisman zijn informatief over lobbyen in het hoogste politieke proces: wie zijn de lobbyisten, hoe gaan ze te werk, hoe komen innige contacten tot stand en wat gebeurt er nu eigenlijk in die achterkamertjes? Er ontstaat een curieus beeld waarin de lobbyisten enerzijds graag transparant zouden willen werken, maar anderzijds goed beseffen dat zij hun werk slechts in vertrouwen, in 'achterkamertjes' kunnen doen. Een vooraanstaande practitioner, Frans van Drimmelen (directeur van één van de grootste Haagse adviesbureaus in public affairs), wordt hierover diepgaand geïnterviewd. 'De kunst van een mooie lobby is niet de ander klemzetten door jouw zin te krijgen, maar samen een maximaal aanvaardbare oplossing vinden. Nederland is klein, je zult elkaar later weer nodig hebben', aldus Van Drimmelen. Discreet samenbrengen, verbinden en bemiddelen blijken de bestanddelen van een succesvolle lobby. De lobbyist opereert als samenwerkingspartner en vertrouweling in een proces waarin politici en bewindslieden publiekelijk hun successen claimen. Anders gezegd, 'Lobbyisten opereren dicht op de macht, er wordt geen politiek besluit genomen zonder dat het een (discreet, A. Wagemaker) stempel draagt van belangenbehartigers.'

Informele macht en invloed

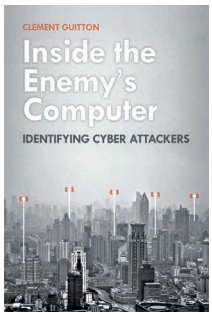
De tweede helft van *Lobbyland* wordt helemaal interessant als Korteweg en Huisman een beeld schetsen van de parallelle Haagse werkelijkheid. De auteurs laten zien hoever de macht van de onzichtbare (lobby-krachten rond het Binnenhof reikt. Er blijken vele informele, *old-boys*-netwerken te bestaan van patriciërs (vooral machtige oud-politici en vooraanstaande figuren uit het bedrijfsleven) die deels onzichtbaar – en dus oncontroleerbaar – werken. Ze weten hoe de hazen lopen en

kennen de mechanismen, waardoor ze effectief en efficiënt kunnen beïnvloeden, zo niet manipuleren. In enige uitgewerkte *cases* wordt duidelijk hoe je de Haagse politiek de gewenste kant op kunt krijgen, hoe het zowel voor als achter de schermen werkt. Het wordt smeuïg als een tipje wordt opgelicht van de bijeenkomsten van de *inner circles* van gevestigde belanghebbenden, zoals de 'Kringen van Lobbyisten', Koning Willem I, II, III en IV. Er is kennelijk een cultuur van impliciete regels die exclusiviteit schragen door de facto te ontkennen dat ze bestaan. Het versterkt de roep om meer transparantie en regulering, maar ook het besef dat achterkamertjes misschien wel nodig zijn. Hoe realistisch dit is laten de schrijvers in het midden. Dat kan ook weinig anders, omdat *Lobbyland* een stevig theoretisch fundament ontbeert. Voor fijnproevers is dit jammer. Maar wie *Lobbyland* heeft gelezen zal geprikkeld zijn meer van de mechanieken te willen weten en de bibliografie van het boek biedt een aardig startpunt.

Voor militairen, zeker zij die werkzaam zijn binnen de Bestuursstaf, is het van belang goed inzicht te hebben in de werking van informele macht en invloed in de politiek. Hoe werkt de Nederlandse lobbyvariant en hoe krijg je invloed in het 'theater van de staat'? *Lobbyland* is functioneel en inspirerend in een tijd waarin we ondervinden hoe vitaal lobbyen is. We ervaren als nooit tevoren hoe complex het is een duurzame, capabele Defensie niet alleen op de agenda van de Tweede Kamer te krijgen en te houden, maar vooral op die van parlementsleden. Ariejan Korteweg en Eline Huisman schetsen een ontluisterend beeld van lobbyen. De lobbyisten zijn tegelijk belangenbehartiger, informatiebron en beïnvloeder (of misschien wel manipulator). Zeker op het politieke niveau gaat het om een elite, een selecte groep van vertrouwelingen met grote informele invloed. Ze werken buiten de spotlights, al hebben ze soms formeel ook publieke invloed. Lobbyen hoort bij een democratie, maar de manier waarop het gebeurt doet sterk denken aan een regentencultuur. Dat lijkt hard aan een grondige revisie toe, maar de vraag blijft hoe. ■

Dr. drs. Allard Wagemaker MA, kolonel der mariniers

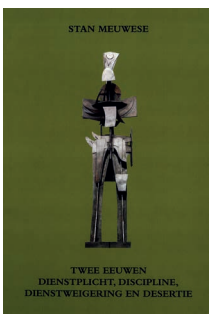
SIGNALERINGEN



Inside the Enemy's Computer

Identifying Cyber Attackers
Door Clement Guitton
Londen (Hurst & Company) 2017
225 blz.
ISBN 9781849045544
€ 30,-

Was het een misdaad, een oorlogsdaad of terreur? De sporen na een cyberaanval kunnen naar uiteenlopende daders of verantwoordelijken leiden en in tegenstelling tot wat vaak wordt aangenomen is cyber crime niet per definitie onoplosbaar. Clement Guitton, voormalig analyst bij het Zwitserse ministerie van Defensie, beschrijft in *Inside the Enemy's Computer* de attributieprocessen na cyberaanvallen. Hij analyseert juridische, technische en politieke aspecten en de stappen die beleidsmakers moeten nemen als de nationale veiligheid in het geding is. Guitton besteedt ook aandacht aan de historie van cyberaanvallen en argumenten bij het ontkennen van verantwoordelijkheid.



Twee eeuwen dienstplicht, discipline, dienstweigering en desertie

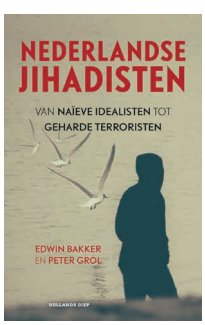
Deelnemen (of niet) aan de Nederlandse krijgsmacht in rechtshistorisch perspectief
Door Stan Meuwese
Oisterwijk (Wolf Legal Publishers) 2017
932 blz.
ISBN 9789462403635
€ 55,-

De Nederlandse wetgever is er nooit in geslaagd een rechtvaardig systeem voor de dienstplicht te ontwerpen. Dat concludeert Stan Meuwese in *Twee eeuwen dienstplicht, discipline, dienstweigering en desertie*, een disseratie aan Tilburg University. Meuwese begint zijn analyse van de ontwikkeling en toepassing van de wetgeving in 1811, vanaf de invoering van de dienstplicht door Napoleon. Hij eindigt bij de opschorting van de dienstplicht en de opkomst van de laatste dienstplichtigen in 1996. Rijken konden in de negentiende eeuw een plaatsvervanger betalen, terwijl in de twintigste eeuw maar één op de zes van een leeftijdsgroep in dienst hoefde en de rest was vrijgesteld, concludeert de auteur.

Religie in conflict

Door Fred van Iersel (red.)
Delft (Academische Uitgeverij Eburon) 2017
148 blz.
ISBN 9789463010924
€ 20,-

Religie in conflict is het eerste deel uit de reeks *Religie en Veiligheid*, opgezet vanuit de Rooms Katholieke Geestelijke Verzorging bij de krijgsmacht, maar bedoeld voor een bredere doelgroep. Eén van de kwesties die auteurs in het boek aan de orde stellen is of levensbeschouwingen bijdragen aan veiligheid, of deze juist bedreigen. Tevens gaan zij in op de veranderde militaire en culturele context van de geestelijke verzorging. Hoe moeten geestelijk verzorgers functioneren in een krijgsmacht die de laatste jaren zwaar onder druk heeft gestaan van bezuinigingen, terwijl er wel deelgenomen werd aan voor militairen in meerdere opzichten zware buitenlandse missies?



Nederlandse jihadisten

Van naïeve idealisten tot geharde terroristen
Door Edwin Bakker en Peter Grol
Amsterdam (Hollands Diep) 2017
256 blz.
ISBN 9789048836444
€ 19,99

Wat drijft Nederlandse jihadisten richting de strijd in Irak en Syrië en welk gevaar gaat er van hen uit? Edwin Bakker, hoogleraar terrorismestudies en Peter Grol, islamoloog, gaan op zoek naar een antwoord in hun boek *Nederlandse jihadisten*. Zij beschrijven acht jongeren die een proces van radicalisering doormaakten en constateren dat de beweegredenen divers zijn. Bakker en Grol vinden dat de maatschappelijke discussie over jihadisten meer kennis en nuance kan gebruiken. Het debat is volgens hen te veel gericht op de mogelijke terugkomst van jihadisten en mogelijke aanslagen en te weinig op push- en pullfactoren en de misdaden die uitreizigers in het Midden-Oosten plegen.

Masteropleiding *Military Strategic Studies* aan de NLDA

De Faculteit Militaire Wetenschappen verzorgt een modulaire Engelstalige wetenschappelijke Masteropleiding (MA). Deze erkende en geaccrediteerde opleiding, *Military Strategic Studies*, start weer in september 2017.

De breed opgezette master bestudeert de rol van het militaire instrument binnen de context van hedendaagse veiligheidspolitieke vraagstukken. De master bestaat uit vier verplichte courses. Daarnaast dienen studenten een keuze te maken uit één van de drie afstudeerrichtingen (tracks) van elk vier courses:

- War Studies
- Intelligence & Security
- Military Management & Logistics

De tracks worden gecompleteerd met een elective. Het volgen van één of meer losse courses (elk 5 EC) is ook mogelijk. U ontvangt na positieve afronding een internationaal erkend academisch certificaat.

De inhoud

De master geeft een grondig inzicht in de functie van krijgsmachten in diverse soorten contemporaine conflicten. Het gaat om conventionele oorlogen zoals *Iraqi Freedom*, etnische conflicten en burgeroorlogen zoals in de Balkan, optreden als onderdeel van een diplomatiek offensief zoals tijdens *Allied Force* boven Kosovo, of inzet ten behoeve van *statebuilding* zoals in Afghanistan. Daarbij komen de politieke, maatschappelijke en wetenschappelijke analyses, debatten en theorievorming aan de orde, evenals de juridische en ethische vraagstukken rond legitimering van militair optreden.

Verder besteedt de studie aandacht aan de interne managementdynamiek van defensieorganisaties en de positie van krijgsmachten binnen moderne westerse maatschappijen. Naast logistieke thema's wordt ook stilgestaan bij de economische en psychologische dimensie van het krijgsbedrijf. Diverse courses gaan over militaire innovatie en de vorming van defensiebeleid. De track *Intelligence & Security* behandelt de rol van inlichtingen en inlichtingenorganisaties en hun betekenis voor het veiligheidsbeleid en militair optreden. Twee voorbeelden van een elective die wordt aangeboden zijn *Cyber Warfare* en *Decision making*.

Zelfstudie

De master, die in deeltijd en modulair wordt verzorgd, kent een aanzienlijke zelfstudielast. De colleges van de tweejarige opleiding vinden op vrijdag plaats op het Kasteel van Breda en zijn opgedeeld in courses van tien weken. De master heeft een omvang van 60 EC en de behaalde studiepunten blijven zes jaar geldig om de operationele flexibiliteit zo veel mogelijk ten goede te komen.

De master is in eerste instantie bedoeld voor militairen en burgers met een bacheloropleiding (of lang model KIM/KMA) en (voor militairen) circa vijf jaar werkervaring in een militaire context. Naast medewerkers van Defensie, de Algemene Inlichtingen- en Veiligheidsdienst en het ministerie van Buitenlandse Zaken, is de master ook zeer geschikt voor bijvoorbeeld medewerkers van ontwikkelingsorganisaties die vanwege hun werk met militaire organisaties samenwerken. Daarnaast kunnen ook andere geïnteresseerden met minimaal een (relevante) bacheloropleiding zich aanmelden.

Voor defensiemedewerkers (militairen en burgers, uit Nederland en NAVO-landen) wordt de studie (vooralsnog) bekostigd door de organisatie. Civiele studenten betalen collegegeld. De master start in principe met maximaal 45 studenten, van wie er circa vijftien van buiten Defensie afkomstig zijn.

Meer informatie

De website van de NLDA (intra- en internet) geeft meer informatie over de inhoud, opzet en toelatingseisen van deze master. De inschrijving voor de master MSS Class 2017 loopt van 1 februari tot en met 30 april.

Informeer ook tijdig bij uw P&O-functionaris. Belangstellenden kunnen nu al mailen naar master.mss@mindef.nl.