Jaargang 189 nummer 9 – 2020

MILITAIRESPECTATOR

INFORMATION MANOEUVRE

THEMANUMMER

Vooruitblik

In *Militaire Spectator* 10-2020 verschijnt onder meer: ‘De Afrikaanse Unie. Een kort verhaal voor denkers in lange lijnen’ van luitenant-kolonel Leen van Hijum.

Hoe het er precies uit gaat zien is moeilijk te zeggen, maar Afrika zal één van de bepalende factoren zijn voor de toekomst van Europa, ook op het gebied van vrede en veiligheid. De Afrikaanse Unie (AU), waarvan alle Afrikaanse landen lid zijn, speelt op dit gebied een centrale rol. Het Peace & Security Department, politiek aangestuurd door de Peace & Security Council, houdt zich bezig met alle fasen van een conflict: conflictpreventie, bemiddeling, interventie en vredesopbouw. Maar de praktijk is weerbarstig. Op politiek niveau is het erg moeilijk om de lidstaten op één lijn te krijgen, de aansturing van AU-missies is problematisch, het overheidsapparaat functioneert gebrekkig. Desondanks is de AU een actor die ertoe doet, wat ook de VN, EU en NAVO onderkennen. Als vrede en veiligheid in Afrika en Europa het Westen een zorg zijn, is investeren in een partnerschap met de AU geen overbodige luxe. ■

FOTO AFRIKAANSE UNIE

MEDEDELING KVBK

KVBK-lid? Geef uw e-mailadres door aan de ledenadministratie

Van veel KVBK-leden ontbreekt het e-mailadres nog in de ledenadministratie. Het doorgeven van een e-mailadres kan via http://www.kvbk.nl/e-mailadres-kvbk-lid of door de hier afgebeelde QR-code te scannen. De KVBK gebruikt e-mailadressen alleen om leden te informeren over verenigingszaken en deelt ze niet met derden.

KVBK
KONINKLIJKE VERENIGING TER BEOEFENING VAN DE KRIJGSWETENSCHAP

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

Secretaris en ledenadministratie
Majoor R. Verheijen MA
E secretaris@kvbk.nl
Nederlandse Defensieacademie (NLDA)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
E 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
Coco Bookmedia

DRUK
Wilco Meppel
ISSN 0026-3869

Coverfoto: Foto Duke University

MILITAIRESPECTATOR

En verder:

Manoeuvreren in de informatieomgeving

Sun Tzu zei: 'Het toppunt van bekwaamheid is het onderwerpen van de vijand zonder te vechten.'[1] Los van het feit dat hij dit waarschijnlijk in het Mandarijn heeft gezegd is de strekking ervan om eerst de plannen van de tegenstander te corrumperen of een wig te drijven in zijn allianties, en pas in laatste instantie het leger zelf of zijn versterkte steden aan te vallen. Het voorbeeld is wat archaïsch, maar Sun Tzu had dan ook nog geen smartphone of internet. Wel was hij zich al bewust dat de tegenstander behalve op een fysieke ook op een cognitieve wijze kon worden overwonnen, ofwel het beïnvloeden van de begripsvorming en interpretatie van de omgeving, de perceptie van een opponent, en het daaropvolgende besluitvormingsproces.

De militaire voorliefde om het kabinet van dode denkers als Sun Tzu en Von Clausewitz te berde te brengen is om duidelijk te maken dat oorlogvoeren gestoeld is op principes – de *nature of warfare*, zoals ook door deze denkers verwoord. En daar waar de omgeving, het materieel en de techniek in de samenleving of bij de krijgsmachten veranderen, verandert ook het karakter van de oorlog. Maar de basisprincipes blijven hetzelfde omdat die gebaseerd zijn op menselijk gedrag: denk daarbij aan het opleggen van de wil aan een opponent, of aan de principes van initiatief en het uitbuiten van een situatie.

De truc is nu om ons militair vermogen aan te passen aan de veranderende omgeving terwijl we de principes niet verloochenen. En dat is gemakkelijker gezegd dan gedaan omdat in onze hoofden het karakter en de principes van oorlogvoeren vaak verweven zijn. Het is niet meer dan menselijk dat militairen terugvallen op beproefd materieel of doctrinaire wijzen van optreden en dat verwarren met principes. En terwijl we zien dat de omgeving verandert laten we kansen liggen, vallen we terug op het vertrouwde platformdenken en stellen ons wellicht bloot aan onvermoede gevaren.

Dat de omgeving en daarmee het karakter van oorlogvoering verandert valt niet meer te ontkennen. De grootste wijziging is de digitalisering van de samenleving, met name het internet en sociale media, die zelfs als 'wapen' worden ingezet, tijdens een conflict of om een conflict te veroorzaken. En niet alleen door een staat, maar door eenieder met een internetaccount, zoals bleek bij de recentelijk gehackte Twitter-accounts van mensen als Elon Musk, Bill Gates en Jeff Bezos.[2] De digitalisering heeft de informatieomgeving niet enkel toegankelijker gemaakt, maar ook exponentieel verruimd. Het gevolg is dat de opponent niet alleen in de fysieke, maar ook in de cognitieve en virtuele dimensie bedwongen moet worden. Het heeft immers weinig zin een conflict met zwaar

1 Vrij vertaald vanuit het Engels, zie: Ralph D. Sawyer, *Sun Tzu. Art of War* (Boulder, Westview Press, 1994) 177.

2 Marc Hijink, 'De hack van Twitter toont aan: zo makkelijk is het sociale netwerk te manipuleren', in: *NRC Handelsblad*, 16 juli 2020. Zie: https://www.nrc.nl/nieuws/2020/07/16/de-bitcoinhack-toont-aan-zo-makkelijk-is-twitter-te-manipuleren-a4006147.

militair materieel in te gaan terwijl je commando-voeringssysteem is gehackt, of als interventiemacht de bevolking te steunen terwijl je niet weet wat hen drijft.

Ook in de *Brede Maatschappelijke Heroverwegingen*,[3] nota bene van het ministerie van Financiën, is bij het thema 'Veiligheid en veranderende machtsverhoudingen' ruim aandacht voor de nieuwere veiligheidsdomeinen: informatiegestuurd optreden, cyber en conflictpreventie. Digitalisering is hierbij een centraal en 'dwarsdoorsnijdend' thema.

Hans van Dalen geeft in dit themanummer van de *Militaire Spectator* aan dat de informatieomgeving niet langer enkel uit de fysieke, maar tevens uit een virtuele en een cognitieve dimensie bestaat. Maar militair optreden in de informatieomgeving om de cognitieve dimensie te beïnvloeden is niet nieuw. De Sovjet-Russische *active measures* bestaan als sinds het begin van de vorige eeuw, zo laat Han Bouwmeester zien in zijn artikel over desinformatie in Litouwen. De digitalisering heeft de informatieomgeving echter wel danig veranderd, wat ook effect heeft op het vergaren van inlichtingen en het verkrijgen van begrip en kennis, maar bovenal tijdens defensief en offensief optreden in die informatieomgeving – de essentie van het concept informatiegestuurd optreden.

Optreden in de informatieomgeving vervangt echter geenszins het traditionele militaire optreden. Het komt ernaast te staan: het is een 'en-en'-variant die het instrumentarium van de krijgsmacht verbreedt. Uiteraard blijven de principes van oorlogvoering overeind, wat inhoudt dat de krijgsmacht – mocht zij worden ingezet voor optreden in de informatieomgeving – een relatief voordeel moet verkrijgen ten opzichte van de partij wier houding of gedrag zij wil beïnvloeden. Het uitbuiten van de mogelijkheden die de informatieomgeving biedt is hierin cruciaal. Information Manoeuvre is daarmee het toepassen van de manoeuvrebenadering in de informatieomgeving.

Dit themanummer van de *Militaire Spectator* geeft inzicht in de impact van de informatieomgeving, vooral bij de krijgsmacht. De informatieomgeving – en met name het digitale segment – is een zegen voor velen, maar ook een vloek met een donkere, corrumperende werking. Beïnvloeding via sociale media, via de virtuele persoonlijkheden van mensen, is voor menig actor een geliefd 'wapen' geworden. Informatie als wapen kent inmiddels vele verschijningsvormen, zoals desinformatie of het manipuleren met beelden (Imagefare) om de cognitieve dimensie, onze perceptie en ons wereldbeeld te beïnvloeden, zoals Bo van den Herik e.a. en Sterre van Hout in hun artikelen illustreren.

Maar de verdediging tegen of de inzet van informatie als wapen blijkt nog niet zo eenvoudig. Hoe verweer je je tegen de alternatieve feiten in een tijdperk van *post-truth politics*? Hoe maak je een samenleving weerbaar? En anderzijds, hoe zet je informatie in als tactisch wapen? Kennis en perceptie van de omgeving en de lokale bevolking vergroot de effectiviteit van de eenheid. Joris van Esch en Simon Hirst belichten de mogelijkheden en onmogelijkheden daarvan vanuit het perspectief van 1 (German/Netherlands) Corps.

De informatieomgeving gaat niet meer weg, maar wordt enkel groter en belangrijker. Het ultieme doel van de krijgsmacht is om relevant te zijn en in staat een opponent te beïnvloeden in de fysieke, virtuele en cognitieve dimensie. Maar we zijn er nog lang niet. En de grootste valkuil is dat we bij het denken over het militaire vermogen in de informatieomgeving toch weer terugvallen op vertrouwde karakteristieken, in plaats van de principes van oorlogvoering. In hun essay geven Gwenda Nielen en Roel Samson op scherpe wijze aan dat het verkrijgen van een relatief voordeel, van initiatief en het uitbuiten in de informatieomgeving andere grootheden kent en niet primair gericht is op de materiële kant van het militair vermogen. Het zit ook in hoe wij optreden, maar bovenal is dit een vraagstuk van mentaliteit: daar zit de echte *capability gap*. ■

3 Kamerstuk II 2019-20 II 32 359 no. 4, Ministerie van Financiën, 'Kamerbrief Brede Maatschappelijke Heroverwegingen', 2020.

On mind war

Manoeuvreren op het internetslagveld

Deze tijd brengt vanwege de nieuwe disruptieve informatietechnologie grote veranderingen met zich mee. Meer en nieuwe spelers betreden het gevechtsveld, vooral online. Op het digitale *battlefield of information warfare* zijn nieuwe wapens nodig. Vooral sociale media bieden ongekende mogelijkheden voor het beïnvloeden van een grote diversiteit aan doelgroepen om missiedoelstellingen naderbij te brengen en het militaire vermogen en de (rechts)staat te beschermen. De spelregels van oorlogvoering veranderen snel en informatie wordt het wapen van de toekomst, of is het eigenlijk nu al. Hoog tijd dat Defensie zich hier rekenschap van geeft en maatregelen neemt, met Information Manoeuvre in het middelpunt. Dit artikel beoogt het inzicht in Information Manoeuvre te vergroten.

Kolonel Hans van Dalen[*]

Informatie wordt al eeuwenlang gebruikt voor beïnvloeding, maar sinds de introductie van smartphonetechnologie is dat explosief toegenomen. Beïnvloeding vindt niet langer uitsluitend plaats via traditionele media zoals kranten, radio en tv, maar vooral via internet en sociale media, met gebruik van geavanceerde technieken.[1] Ook zijn het niet langer statelijke actoren of adverteerders die geraffineerde beïnvloedingsmethoden gebruiken, maar ook niet-statelijke groeperingen zoals belangengroeperingen, non-profit organisaties, milities en criminele organisaties of individuen. Er is een ware omwenteling veroorzaakt door moderne vormen van informatietechnologie, die niet alleen bedreigingen voor de stabiliteit van de westerse samenleving met zich meebrengen, maar ook kansen.

Om te analyseren welke gevolgen de veranderde informatieomgeving heeft voor het militair vermogen, begin ik dit artikel met een korte duiding van de relatie tussen veranderingen in informatietechnologie en veranderingen in de maatschappelijke ordening. Daarna behandel ik een tweetal trends die het gevolg zijn van informatietechnologie, waarbij ik ook aandacht schenk aan de corrumperende werking van informatie. Zonder dat te herkennen, worden wij immers dagelijks geconfronteerd met de nadelen van informatie. Vervolgens maak ik een stap naar het militaire werkveld en leg ik uit hoe de informatieomgeving is opgebouwd en hoe daarbinnen gemanoeuvreerd kan worden. Daarna doe ik voorstellen hoe Defensie met deze veranderingen kan omgaan en waar de kansen liggen. Het artikel eindigt met een korte samenvatting van de belangrijkste zaken. Het doel van dit artikel is bij te dragen aan de verdieping van het Information Manoeuvre-gedachtegoed binnen en buiten Defensie.

De veranderde informatieomgeving heeft gevolgen voor het militair vermogen en dat vereist meer inzicht in het concept Information Manoeuvre

FOTO MCD, JARNO KRAAYVANGER

[*] Kolonel van Dalen is regimentscommandant Huzaren van Boreel en maakt deel uit van de staf van de Koninklijke Landmacht. Dit artikel is op persoonlijke titel geschreven en geen defensiebeleid. De auteur bedankt kolonel Peter Pijpers voor zijn commentaar op de oorspronkelijke tekst.

1 B.M.J. Pijpers, 'De twitterende tegenstander. Een discours over de rol van mediaculturen in een conflict', in: *Militaire Spectator* 183 (2014) (6) 300-314.

Moderne informatietechnologie kent veel voordelen, maar draagt ook het gevaar van ontwrichting van maatschappijen in zich

De ontwikkeling van de informatietechnologie

Door razendsnelle ontwikkelingen in de informatietechnologie en de verspreiding van internet onder de wereldbevolking is het mogelijk informatie onder meer te gebruiken om sociale verbanden te vormen, te beïnvloeden of te ontwrichten. Zelfs staatsvormen kunnen worden ontwricht. Informatietechnologie wordt meer en meer beschouwd als een *weapon of mass disruption.* Sommigen spreken al van *virtual societal warfare*.[2] Significante veranderingen in informatietechnologie hebben echter altijd al een belangrijke rol gespeeld bij maatschappelijke omwentelingen in de geschiedenis.[3] Denk daarbij aan de introductie van de boekdrukkunst, kranten en later telegrafie, radio en de tv. Macht is namelijk voor een gedeelte gestoeld op toegang tot informatie en veranderingen in vorm, omvang en snelheid van informatie hebben vaak geleid tot periodes van politieke instabiliteit met volksopstanden, revoluties en oorlogen tot gevolg.

Met de introductie en de wereldwijde verspreiding van computers en (later) internet, begin jaren negentig, kwam de volgende golf van veranderingen op gang. De Age of Computers was aangebroken. Informatie begon van letters, audio en beeld in data te veranderen: van analoog naar digitaal. De mogelijkheden tot snelle wereldwijde informatie-uitwisseling en samenwerking leidden tot grote handelsstromen, welvaartsstijging en hoop op een betere wereld. Maar niet alleen dat. Door de toenemende processorcapaciteit, het verkleinen en het dematerialiseren van data[4] zijn mensen met de introductie van smartphonetechnologie meer verbonden, communicatiever en betrokkener dan ooit tevoren.[5]

De schaduwzijde van informatie

Maar behalve voordelen kent informatie ook negatieve aspecten en een 'donkere, duistere' zijde. Sommige van deze negatieve aspecten zijn duidelijk waarneembaar, maar sommige liggen dieper onder de oppervlakte en vragen om meer studie. Aan de hand van twee trends, die ook militaire relevantie hebben, beschrijf ik daarom enkele negatieve gevolgen van informatie die een impact hebben op democratische samenlevingen.

De eerste trend is de exponentieel uitgebreide mogelijkheid van mensen voor interactie met elkaar. Deze interactie kan allerlei vormen hebben, van transacties en kennisproductie tot onderzoek en fysieke samenwerking en het is gemakkelijker geworden voor mensen om grensoverschrijdend te kunnen samenwerken. Daardoor ontstaan er spontaan veel zelfregulerende wereldwijde netwerken, die soms staatsbeleid ondersteunen, maar dat vaak ook verstoren en zelfs belemmeren. Naim geeft aan dat verticale controlestructuren (zoals staat, vakbonden en bureaucratische organisaties) aan belang en macht verliezen ten gunste van horizontale samenwerkingsverbanden in netwerken.[6] Belanghebbende netwerken, die steeds moderne blockchainconcepten gebruiken voor onderlinge transacties en staatsorganisatie niet meer nodig hebben, dringen traditionele regeringswerkvelden binnen, zoals zorg, infra-

2 Zie Michael J. Mazarr e.a. (red.), *The Emerging Risk of Virtual Societal Warfare. Social Manipulation in a Changing Information Environment* (Santa Monica, RAND Corporation, 2019).

3 Antoine Bousquet, 'Chaoplexic Warfare or the Future of Military Organization', in: *International Affairs* 84, No. 5 (2008) 915-29 (915-918). Zie: https://doi.org/10.1111/j.1468-2346.2008.00746.x.

4 Roy van Keulen, *Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age* (Dissertatie Universiteit Leiden, 9 mei 2018) 20.

5 Bill Gertz, *iWar. War and Peace in the Information Age* (New York, Threshold Editions, 2017) 23.

6 Moises Naim, *The End of Power. From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What It Used to Be* (New York, Basic Books, 2013).

structuur, onderwijs en veiligheid. Energieke individuen kunnen deze netwerken razendsnel en wereldwijd opzetten. Met andere woorden, *the empowerment of the individual* is een belangrijke trend, die het belang, nut en daarmee de legitimiteit van de staat ondergraaft. En deze empowered individual speelt ook een steeds grotere rol op het slagveld.

De tweede belangrijke trend is dat het publiek niet langer uitsluitend nieuwsconsument is, maar eveneens nieuwsproducent. Dit wordt ook wel *produser* (*user who can also produce content*) of *citizen journalism* genoemd.[7] Deze trend, meer nog dan de eerste, is de grootste verandering in de wereld. Mensen kunnen nu wereldwijd berichten verspreiden, met één klik en zonder wezenlijke kosten. Deze zaken veranderen de productie, vorm, inhoud en consumptie van alle soorten media.[8] Traditionele media (kranten, radio en tv) reageren hierop door samen te gaan met 'nieuwe' mediabedrijfjes, gespecialiseerd in sociale media.[9] Een ander fenomeen is de clickratio. Het verdienmechanisme van veel socialemediabedrijven is namelijk gebaseerd op het aantal clicks per *post* en de opbrengsten stijgen als posts viraal gaan. En 'viraliteit' hangt rechtstreeks samen met 'sensationalisme',[10] wat bereikt kan worden met beangstigende, bloederige, seksueel-getinte of anderszins indrukwekkende beelden. Het gevolg is dat informatie niet langer een rol lijkt te spelen bij waarheidsvinding. Objectieve waarheid bestaat niet meer. De hedendaagse mensheid leeft in een *post-truth age* en zoekmachines bepalen onze nieuwe waarheden. Erger nog: we zijn helemaal niet meer geïnteresseerd in waarheid. Mensen zijn op zoek naar aandacht en sensatie en deze drang is moeilijk te beteugelen, temeer omdat het veelvuldig herhalen van de content de overtuigingswaarde ervan vergroot, zelfs als het een leugen is. Sinds we weten dat digitale informatie zeer vluchtig is en gemakkelijk kan worden gemanipuleerd of veranderd, vertrouwen mensen bovendien de informatie zelf ook niet meer.[11]

Deze twee trends hebben gevolgen voor de defensieorganisatie. Oorlog is gedemocratiseerd en van ons allemaal. Oorlog is niet langer een voortzetting van politiek. Oorlog is nu allemanspolitiek geworden. Het slagveld wordt meer en meer betreden door niet-militaire actoren, die zich via de smartphonetechnologie en internet actief met de gevechten bemoeien.[12] Velen indirect en op afstand, maar sommigen direct en in de fysieke nabijheid. Deze deelname kan diverse vormen aannemen, van het vergroten of verminderen van draagvlak onder bevolkingsgroepen[13] tot het organiseren van fysieke logistieke ondersteuning; van het rekruteren en trainen van milities tot virtuele massarekrutering (*army of hackers*); van het vergroten van de weerbaarheid van de eigen bevolking tot het uitvoeren van online-inlichtingenoperaties (zoals het Bellingcat-collectief[14] of het gerenommeerde socialemedia-analysebedrijf Meltwater); van het doen van technologisch onderzoek tot het online gezamenlijk fabriceren van wapens. Ook de Nederlandse krijgsmacht maakt stappen op dit gebied en maakt gebruik van door de civiele markt aangeboden onderzoeks- en analysemethodieken.[15]

7 David Patrikarakos, *War in 140 Characters. How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York, Basic Books, 2017) 20 e.v.

8 Zie: Mazarr, *The Emerging Risk of Virtual Societal Warfare*, hoofdstuk 2: 'The Evolving Infosphere'.

9 Ibid, 25, 28.

10 Ibid, 23.

11 Zie: David Bawden en Lyn Robinson, *The dark side of information: overload, anxiety and other paradoxes and pathologies* (Londen, City University of London, 2008) 7. Zij introduceren de begrippen *impermanence of information* en *shallow novelty*. De 'vluchtigheid en 'veranderbaarheid' van digitale informatie vermindert de wetenschappelijke waarde ervan.

12 Zo was het in Libië een 23-jarige vrouw die de coördinaten van Gaddafi's tanks doorbelde, zodat de westerse vliegers wisten waar ze moesten bombarderen. Zie: http://www.newsmax.com/Newsfront/Libya-woman-spy-gadhafi/2011/09/12/id/410590.

13 'Trollen' versus 'Elves'. In reactie op pogingen van Russische en Chinese trollfabrieken om desinformatie te verspreiden is een spontane tegenbeweging ontstaan van onlinegroepen. Deze groepen noemen zich vaak Elven en hebben als doel desinformatie bloot te leggen (engels: *debunk*).

14 Een kleine greep uit belangrijke Bellingcat-onthullingen: locaties waar IS onthoofdingsvideo's opnam, dat vlucht MH17 door een Russische Boek-raket was neergehaald en het ontmaskeren van de verdachten van de gifgasaanval op dubbelspion Sergej Skripal in Engeland.

15 Esther Rosenberg en Karel Berkhout, 'Een soft maar gevaarlijk wapen: moderne oorlogsvoering richt zich op beïnvloeding van de bevolking', (interview met luitenant-generaal Martin Wijnen, Commandant Landstrijdkrachten) in: *NRC Handelsblad*, 26 juni 2020. https://www.nrc.nl/nieuws/2020/06/26/een-soft-maar-gevaarlijk-wapen-moderne-oorlogsvoering-richt-zich-op-beinvloeding-van-de-bevolking-a4004227.

Als gevolg van disruptieve informatietechnologie erodeert de democratie en neemt het vertrouwen in bestaande politieke, financiële, economische, juridische en zelfs maatschappelijke instituties af

FOTO RIJKSOVERHEID, JEROEN VAN DER MEYDE

De overvloed aan informatie werkt echter ook verstorend en ongemerkt maakt het menselijke interacties en vooral besluitvorming vaak langzamer. Daarnaast nemen mensen door de *information overload*[16] informatie slechts vluchtig tot zich en hebben geen tijd of energie meer om diepteonderzoek te doen, misinformatie op te sporen, tegenargumenten te horen of wetenschappelijke studies te raadplegen. De transparantie en de enorme hoeveelheid beschikbare informatie weerhoudt leiders – en commandanten – steeds meer om snelle en tijdige beslissingen te nemen, vooral als deze risicovol zijn. Maar het beschadigt tevens militaire basisvaardigheden. Net zoals in het civiele domein software en apps bestaan die keuzes bepalen (wat we kijken, wat we leuk vinden) en vaardigheden overnemen, is dit ook zo in de militaire wereld. Software bepaalt waarop we schieten, hoe we rijden, hoe we varen, hoe we vliegen, hoe we navigeren, wie we promoveren, hoe groot onze logistieke voorraden moeten zijn, wie en wanneer we bevoorraden, wanneer de slijtage aan onze gevechtsvoertuigen te groot wordt en welke militaire operaties we moeten uitvoeren. Dit is een gevaarlijk fenomeen. Algoritmes bedreigen menselijke vrijheden. Artificial Intelligence (AI) haalt de menselijkheid uit de mens en de strijder uit de soldaat. Militaire eenheden moeten immers (als de connectie wegvalt) ook zonder software en apps nog altijd hun militaire taak kunnen uitvoeren. Maar militairen dreigen hun elementaire vaardigheden hiervoor kwijt te raken.

Als gevolg van deze nieuwe disruptieve informatietechnologie erodeert bovendien de democratie. Het vertrouwen in bestaande politieke, financiële, economische, juridische en zelfs maatschappelijke instituties is beschadigd, mede door de Snowden-onthullingen en Wikileaks-publicaties, waardoor sociaal kapitaal is gecorrodeerd. De bevolking raakt steeds verder

16 Zie: David Bawden en Lyn Robinson, *The dark side of information*. Zij introduceren een aantal *information pathologies* (vreemde manieren om met disruptieve informatietechnologie om te gaan), zoals *information overload, information anxiety, infobesity en satisficing*.

gepolariseerd. Daarbij dreigen de 'openheid van het debat' en 'angst voor media- of publieke veroordeling' de scherpe kanten van de politieke discussie te halen en mensen naar 'politiek correcte' antwoorden en standpunten[17] te drijven, waarmee de gezagscrisis compleet is.[18] Veel belangengroeperingen, industrieën en politici hebben dit ontdekt en beseffen dat ze, om hun doelstellingen te bereiken, hun activiteiten het beste kunnen richten op het vertrouwen en de bestaande polarisatie van de doelgroepen. Soms willen ze het vertrouwen in bestaande zienswijzen beschermen, soms willen ze die veranderen. Openlijk tegenspreken is vaak niet de beste methode, twijfel zaaien over een bestaande zienswijze wel. Denk daarbij aan publicaties over de al dan niet schadelijke effecten van roken, suiker, alcohol en van vuurwapens.[19] Twijfel over de menselijke aspecten van vluchtelingenopvang, armoede, de Covid-19-aanpak en het stikstofbeleid. Twijfel over de regering, twijfel over de doodstraf. Twijfel over alles.

Informatietechnologie is bij uitstek geschikt voor het bevorderen van polarisatie en het zaaien van twijfel. Terwijl het gemak en de reikwijdte van internet en sociale media mensen juist wereldwijd zouden kunnen verbinden, verdelen ze mensen meer en meer in online datagroepen, waardoor mensen uiteen worden gedreven en standpunten verharden. Er is sprake van een *digital divide*.[20] Met de modernste technologieën kunnen beïnvloeders op persoonlijke behoefte afgestelde data genereren: *personalized targeting* of *precision targeting of influence* genoemd. Door gebruik van AI voor automatische dataverzameling, evaluatie en manipulatie en de toepassing van algoritmes voor geautomatiseerde besluitvorming kunnen we gevoed worden met informatie die ons beeld enkel maar bevestigt, de zogeheten *echo chambers* en *silos of belief*. Dit alles wordt steeds omvangrijker doordat informatieplatforms elkaar opkopen en zich concentreren.[21] *The infosphere is not universal, but is becoming fragmented.* Dit is een bedreigende ontwikkeling.

Deze polarisatie en groeiende twijfel raakt de mensheid in de kern. Het vermogen om in grote groepen na te denken stelde mensen immers in staat om voor de meest complexe problemen (honger, armoede en ziekte) oplossingen te bedenken. Terwijl internet de samenwerking juist zou moeten verbeteren, dreigt het groeiend gebrek aan vertrouwen dit tegelijkertijd te verstoren. Polarisatie vindt plaats terwijl er tegelijkertijd grote problemen op de mensheid afkomen, zoals overbevolking, ecologische veranderingen, immigratie en grondstoffenmanagement. In de internationale arena is deze trend te zien. Er wordt internationaal steeds minder samengewerkt en internationale instellingen (Wereldbank, Internationaal Monetair Fonds, Shanghai Cooperation Organization, Verenigde Naties, Europese Unie, NAVO) verliezen allemaal terrein. Veel landen keren in zichzelf en bouwen muren in plaats van bruggen. De recente coronacrisis, de daarop volgende economische crisis en gebrek aan Europese solidariteit lijken dit beeld te bevestigen. In de literatuur worden dan ook steeds meer beangstigende termen gebruikt, zoals *global libertarianism, progressive localism, national protectionism* of *national developmentalism*. Er is een vertrouwenscrisis.

Militair belang van de informatieomgeving en het manoeuvreren daarbinnen

De bovengenoemde (informatie)trends zijn ook van grote invloed bij militair optreden. Recente conflicten hebben al de kracht getoond van veranderende percepties onder de bevolking. Een militaire operatie lijkt niet langer te worden afgemeten aan het behalen van 'militaire doelstellingen', maar aan de perceptie onder de bevolking van de operatie, zeker in de heden-

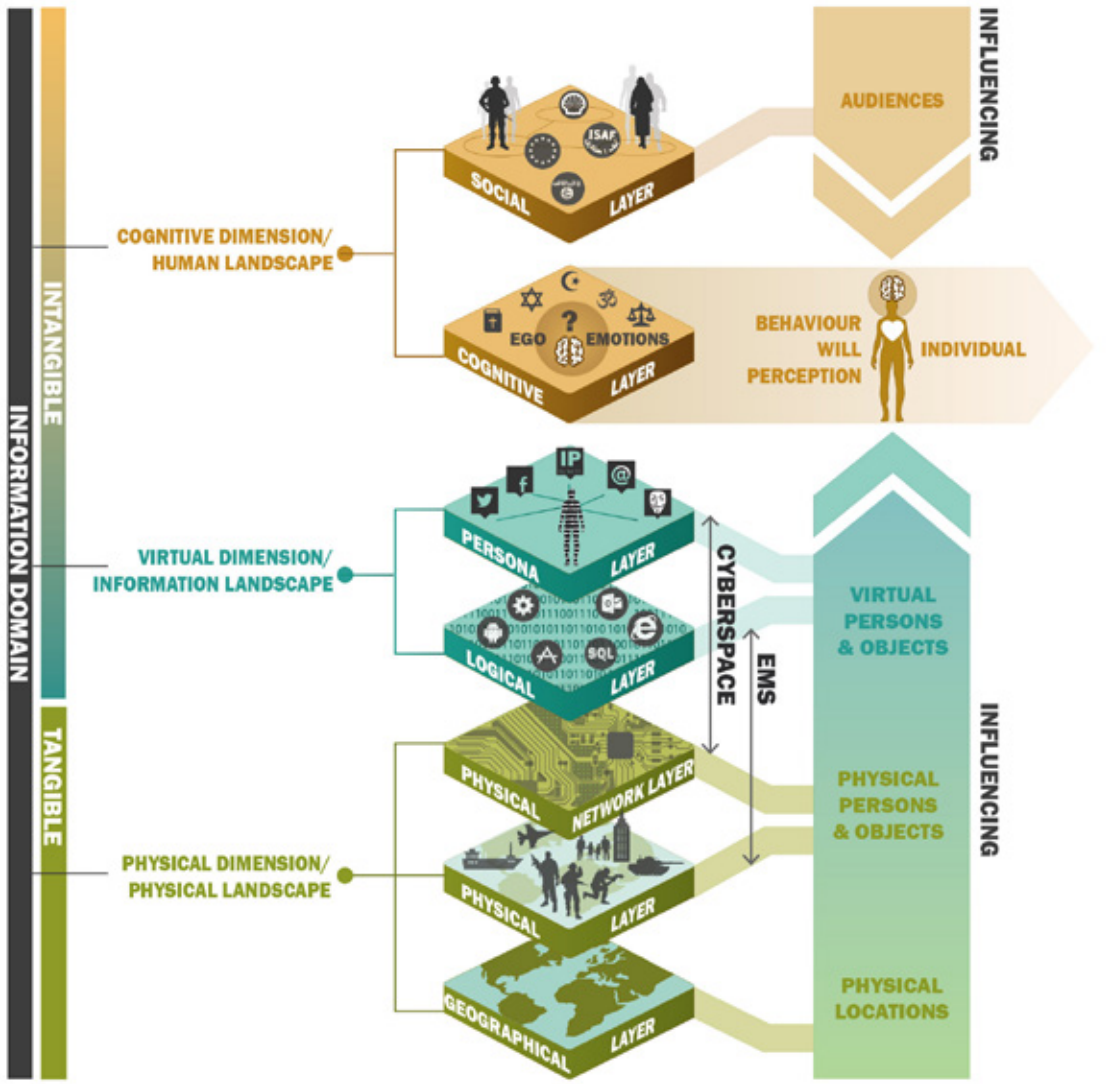
17 Bill Gertz, *iWar,* 'How the US can beat China, Russia, Iran, North Korea and Islamic Terrorists on the Digital Battlefield', 7.

18 En deze 'gezagscrisis' heeft publiek verzet tot gevolg, zoals de gelehesjesbeweging, civiele onrust en de opkomst van populisme.

19 Zie: Naomi Oreskes en Erik M. Conway, *Merchants of Doubt. How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming* (Londen, Bloomsbury, 2012).

20 Bawden en Robinson, 'The dark side of information', 3.

21 Zie: Mazarr, The Emerging Risk of Virtual Societal Warfare, hoofdstuk 2: The evolving infosphere.



Figuur 1 Het informatiedomein

daagse digitale onlinesamenleving. De fysieke operaties lijken ondergeschikt of ondersteunend aan het echte gevecht: de strijd in het informatiedomein. Beeldvorming (en dus informatie) is niet langer ondersteunend, maar *leidend* geworden. Vandaar de termen perceptieoorlogvoering en Information Manoeuvre (Info Man). Informatie is een machtig wapen geworden en met de introductie van de smartphonetechnologie is iedereen een potentiële journalist geworden, of, in militaire termen, een sensor. Maar omdat hij of zij in staat is om rechtstreeks online mee te vechten is hij of zij niet alleen een sensor geworden, maar ook een *weapon*. Veel van deze onlinestrijd is een gevecht met woorden en vooral (sensationele) beelden, maar daarom niet minder schadelijk. Is de socialemediagebruiker daarmee ook een 'strijder' geworden, op wie de oude combattantenregels (georganiseerd, geüniformeerd en bewapend) niet meer toepasbaar lijken te zijn? Is nu iedereen die meevecht ook een 'legitiem' doelwit? Mag een Army of Tweeters, een troll of chatbot onschadelijk worden gemaakt, als we de identiteit van deze virtuele strijders al kunnen achterhalen? De nieuwe ontwikkelingen leiden

tot nieuwe uitdagingen op juridisch, ethisch en financieel gebied, maar dat mag absoluut geen reden zijn om ons hoofd weg te draaien voor de rol van Defensie in het informatiedomein.

Het informatiedomein is, in tegenstelling tot de domeinen zee, land, lucht en ruimte, geen fysiek domein, maar een conceptueel omvattend idee. Een recente studie gebruikt daarom de term *infosphere*[22] en ook in Nederlandse doctrinedocumenten wordt de term informatieomgeving soms gebruikt. Het informatiedomein omvat alles waarin zowel fysieke als niet-fysieke handelingen, activiteiten en 'manoeuvreren' kunnen plaatsvinden. De domeinen cyber (of cyberspace) en elektromagnetisch spectrum (EMS) zijn deel van het informatiedomein.[23]

Het informatiedomein kent drie dimensies: de cognitieve, virtuele en fysieke dimensie. Al deze dimensies bieden aangrijpingspunten voor Information Manoeuvre-activiteiten en moeten aan eigen zijde dus ook worden verdedigd.

Fysieke dimensie
De fysieke dimensie van het informatiedomein omvat alle 'zichtbare' en 'tastbare' elementen die informatie dragen of verzenden. Dit kunnen fysieke objecten zijn zoals satellieten, vlugschriften, kranten, routers, zenders, communicatietorens, apparaten en zelfs menselijke lichamen. De fysieke dimensie kent drie lagen: een *geografische laag* (die aangeeft waar op de aardbol die fysieke zaken zich bevinden), een *fysieke laag* (wat voor soort object het is) en een *netwerklaag* (hoe deze objecten informatietechnisch met elkaar verbonden zijn).

Virtuele dimensie
De virtuele dimensie omvat alle niet-tastbare communicatie van data, informatie, inlichtingen of kennis in alle denkbare vormen, zoals tekst, beelden, metadata, protocollen, algoritmes, EMS-straling. De meeste informatietransmissie vindt tegenwoordig plaats via EMS en cyberspace, hoewel fysieke kranten en boeken ook nog een rol spelen. De virtuele dimensie kent een *persona-laag* (de virtuele identiteit van personen en organisaties in cyberspace en EMS) en een *logische laag* (de data zelf, zoals bits en bytes, data van de socialemediaprofielen en data op de internetsites).

Cognitieve dimensie
De cognitieve dimensie behandelt alle gedachten, emoties, overtuigingen, waarden, normen, percepties en belangen van personen en organisaties. Op deze elementen zijn menselijke emoties immers gebaseerd. Deze elementen zijn niet tastbaar. Ze worden beïnvloed doordat mensen informatie met elkaar delen, dus zowel zenden als ontvangen. Deze onderling communicerende mensen vormen de *sociale laag*. De gedachten, emoties, overtuigen, perceptie, et cetera in de individuele hoofden vormen de *cognitieve laag*. Deze cognitieve dimensie is de belangrijkste dimensie, want ons cognitief (begrijpend) vermogen maakt ons tot mensen en hier vindt ook menselijke besluitvorming plaats, die overigens over het algemeen meer op heuristieken dan op rationaliteit is gebaseerd.[24] Strijd in de fysieke dimensie is er op gericht om ons met militaire dwangmiddelen in de cognitieve dimensie dingen te laten 'voelen' en 'begrijpen'. In de cognitieve dimensie vindt dus uiteindelijk conflictbeslechting plaats en daarom liggen hier kansen voor beïnvloeding met informatie: dit is het belangrijkste aangrijpingspunt van Information Manoeuvre.

De drie dimensies, verdeeld in zeven lagen, vormen gezamenlijk het informatiedomein (of informatieomgeving). Ze bieden meerdere aangrijpingspunten voor civiele en militaire beïnvloedingsactiviteiten, hoewel het onderscheid daartussen is vervaagd. Deze beïnvloedingsactiviteiten kunnen daarnaast fysiek of niet-fysiek zijn. Met het model van het informatiedomein in het achterhoofd kan informatie worden gebruikt om allerlei doelgroepen (tegenstanders, medestanders, *bystanders*) te beïnvloeden. Dit gebeurt door bijvoorbeeld bevoordeling, benadeling, manipulatie, misleiding, verleiding, herhaling,

22 Mazarr, *The Emerging Risk of Virtual Societal Warfare*, 13.
23 Zie voor de Nederlandse militaire visie op het informatiedomein: *Informatie als wapen* (Studie Delphi, CLAS, 2017).
24 Dat is de belangrijkste conclusie van de toonaangevende studie over ons menselijk brein: Daniel Kahneman, *Thinking, Fast and Slow* (New York, Penguin Books, 2012).

Informatie heeft ongekende beïnvloedingsmogelijkheden en is een wapen waarmee een grote verscheidenheid aan doelgroepen kan worden beïnvloed

impressie, dwang, vernietiging, et cetera en zowel openlijk als heimelijk, direct als indirect, met fysieke als met niet-fysieke activiteiten. Activiteiten in één afzonderlijke laag hebben vaak neveneffecten in andere lagen, maar uiteindelijk hebben alle informatieactiviteiten, in welke laag dan ook, een resultaat in de bovenste, cognitieve laag. Alles heeft daarom een effect in het hoofd van mensen. Het gaat hierbij om *begrip* en *perceptie* en om deze twee thema's draait alles bij Information Manoeuvre.

Gelukkig heeft dit ook in de nieuwste *Nederlandse Defensie Doctrine* (NDD) een plaats gekregen, onder de aanduiding 'dimensiemodel'. Het dimensiemodel is volgens de NDD 'een manier van denken om domein-onafhankelijk potentiële effecten en afhankelijkheden van militaire activiteiten binnen de operationele omgeving te duiden. [...] Het dimensiemodel kan verder worden uitgebreid met lagen (omgevingen) en entiteiten. De lagen vormen de context voor militaire activiteiten, terwijl de entiteiten binnen deze lagen aangegrepen kunnen worden door activiteiten en/of operaties.'[25] De NDD erkent het belang van informatie en spreekt ook over beïnvloeding met informatie, maar ziet het slechts als ondersteunend aan fysieke manoeuvre. Information Manoeuvre draait dit om en stelt dat fysieke manoeuvre ten dienste staat van informatiemanoeuvre: perceptie-oorlogvoering is vandaag de dag leidend.

Information Manoeuvre

Met het informatiedomein helder voor ogen kan een verdieping plaatsvinden op het manoeuvreren met informatie. De definitie van Information Manoeuvre is: 'De exploitatie van informatie in al haar verschijningsvormen voor offensieve en defensieve doelstellingen'.[26] Hieruit kunnen in grote lijn twee benaderingen worden afgeleid: een directe en een indirecte.

Directe benadering

De directe benadering vindt vooral plaats in de onderste lagen van het informatiedomeinmodel; vaak in de fysieke dimensie en soms ook in de virtuele dimensie. Bij deze benadering zijn alle activiteiten gericht op het verminderen van het vermogen van een tegenstander om juist en snel met informatie om te gaan. Het is gericht op zijn fysieke informatiesysteem (*destroying and hacking systems*), waarbij tegelijkertijd het eigen vermogen tot informatiehandelen moet worden beschermd. Dit kan bereikt worden door fysieke vernietiging of degradatie van commandoposten, zendmasten, routers, databases, glasvezelkabels, communicatieknooppunten en communicatiesatellieten). Het kan met fysiek geweld, met elektromagnetische-energie (stoorcapaciteit) of cyberactiviteiten (hacks en intrusie). In de *Age of Data* is vernietiging of degradatie van het vijandelijke informatiesysteem effectiever dan de vernietiging van zijn militaire eenheden, zoals reserve-eenheden, artillerie-eenheden of logistieke voorraden. Hier liggen belangrijke dilemma's: sturen we onze kruisvluchtwapens, gewapende drones en bommenwerpers af op wapenfabrieken of op trollfabrieken? Gaan we vijandelijke luchtverdediging hacken of vijandelijke netwerkverdediging?

Indirecte benadering

De indirecte benadering speelt zich af in de bovenste lagen, in de virtuele en cognitieve dimensies. Hier gaat het om beïnvloeding van de geest (*hacking humans*) en er is een grote verscheidenheid aan doelgroepen, zeker omdat iedereen tegenwoordig online kan meevechten. Dat zijn de troepen van de tegenstanders, milities, bevolkingsgroepen, leiders, influencers, bloggers, zijn oppositie, criminele organisaties of

25 *Nederlandse Defensie Doctrine* (Den Haag, miniserie van Defensie, 2019) 82-83.
26 Uit: *Informatie als Wapen*.

zelfs geestelijkheid. Maar ook wijzelf hebben soortgelijke doelgroepen aan onze zijde, die we moeten beschermen tegen vijandelijke misinformatie en beïnvloeding. Maar ook belangrijke wereldwijde doelgroepen moeten we beïnvloeden ten gunste van onze doelstelling. Coalitiepartners, internationale belangennetwerken, geestelijkheid, spirituele leiders, techgiganten, socialemediaplatforms, vitale wapenindustrieën of grondstofeigenaren, filmindustrie, gameplatforms, jeugdleiders en ga zo maar door: alles wat significante invloed kan hebben op het strijdverloop. De partij die het beste de wereldperceptie kan beïnvloeden en naar haar hand kan zetten heeft overduidelijk de beste kansen op succes, met name in het tijdperk van massamedia en citizen journalism.

En hier liggen duidelijk mogelijkheden, die Defensie moet benutten. Mensen vertonen vaak vaste patronen in hun gedrag.[27] Dit is een mechanisme dat ervoor zorgt dat mensen in een complexe omgeving automatisch handelen om tijd en energie te sparen of om snel te kunnen reageren bij gevaar. Dit handelen gebeurt vaak op basis van beperkte informatie of signalen. We kunnen daarom onbewust handelen en gedrag beïnvloeden door 'doelgericht' meer informatie te geven. Dit doelgericht beïnvloeden is het meest effectief als wordt ingespeeld op sociaal-culturele principes die verleiden tot instemming met een voorstel. Er zijn een paar basisprincipes om succesvol te zijn, zoals het gebruik van sociale bewijskracht (instemmen met de heersende mening van de groep waar je toe behoort, kuddegedrag), inspelen op sympathie (instemmen met sympathieke personen) en autoriteit (instemmen met meningen van mensen met autoriteit). Deze principes zijn effectief doordat ze gebruik maken van het onbewuste (reflex)handelen van mensen.

27 Zie: Majoor Maarten Gortworst, *Sociale media als wapen. De inzet van sociale media als beïnvloedingsinstrument tijdens militaire operaties* (Thesis, NLDA, 2019) en Robert B. Cialdini, *Influence: Science and Practice* (5th edition) (Londen, Pearson Education, 2009).

De NDD spreekt ook over beïnvloeding met informatie, maar ziet het slechts als ondersteunend aan fysieke manoeuvre; Information Manoeuvre draait dit om

FOTO MCD

Maar deze indirecte benadering, het beïnvloeden van de geest, is niet zo eenvoudig. Het is immers moeilijk om een perceptie uit iemands hoofd te krijgen, zeker als het om identiteit gaat. En toch zijn hiervoor een paar methodes. Ten eerste is snelheid van belang. Een snel, maar onjuist of onvolledig bericht, heeft vaak veel grotere invloed dan trage, juiste berichten. Een vaak herhaalde leugen wordt een waarheid. Tegelijkertijd worden op de lange termijn wel leugens ontmaskerd door online waarheidsbevindingen, dus te veel openlijk liegen werkt op de lange termijn contraproductief.
De inhoud is ook belangrijk, want sensationele berichten gaan sneller viraal dan saaie berichten. Het gaat ook om de vorm – beelden zijn belangrijker dan woorden – en de verpakking, zoals kleuren, omlijstingen, bewegingen, vormen en zelfs geuren. Verder gaat het om het platform – sommige zijn beter geschikt dan andere – om timing en context – op welk moment (dag of nacht) en tegen welke algemene achtergrond of algemene tendens is een bericht het meest effectief? – en om volume, want als een bericht op meerdere manieren veel in het nieuws komt worden mensen hierdoor beïnvloed. Daarnaast speelt ook herhaling een belangrijke rol: een frequent herhaald bericht vormt op zichzelf ongemerkt een waarheid.

Het primaire doel van Information Manoeuvre is om doelgroepen bij de tegenstander te beïnvloeden door twijfel te zaaien, vertrouwen te ondermijnen, breukvlakken bloot te leggen, ideologieën tegen te spreken, oppositie te versterken, zijn leiders in diskrediet te brengen en het draagvlak voor militair optreden te verminderen. Daarnaast moet voorkomen worden dat een tegenstander bij ons hetzelfde doet. Tegelijkertijd kunnen we neutrale bijstanders overhalen ons te steunen met hun online activiteiten.

Los van de vraag of het mag, kunnen we nu al veel. Van de klassieke propaganda en desinformatiecampagnes tot het fabriceren van gemanipuleerde video's en audio-berichten of het binnendringen en verstoren van vijandelijke economische, sociale en economische databases, en vijandelijke algoritmes voor besluitvorming aanpassen of vertragen. Dit alles is gericht op het vergroten van de breukvlakken in de vijandelijke samenhang en het verminderen van zijn vermogen om met informatie om te gaan. Als we deze methodieken projecteren op het informatiedomein kunnen we in het fysieke domein vanzelfsprekend vooral fysieke benaderingen toepassen of cyberaanvallen, gericht op degradatie van systemen. In het virtuele domein liggen Elektronische Oorlogvoering (EOV), tactische Signals Intelligence (SIGINT) en tactische cyber (Cyber Elektro Magnetic Activities, CEMA) als instrumenten meer voor de hand. En in het cognitieve domein moeten beïnvloedingsactiviteiten worden uitgevoerd gericht op cognitieve degradatie van (interactie tussen) mensen.

Wat moet Defensie doen?

Maar wat zou onze defensieorganisatie moeten doen? Om te beginnen moet het socialemediaslagveld niet zonder slag of stoot worden prijsgegeven. Naast luchtverdediging, kustverdediging of grondgebiedverdediging moet de Nederlandse defensieorganisatie ook meehelpen de verdediging te organiseren tegen ongewenste beïnvloeding en daarmee de geesten van de bevolking (en de leiders) beschermen. En niet alleen focussen op verdedigen (*defend, deny, reconnect, repair*) tegen beïnvloeding, maar ook inlichtingen verzamelen over beïnvloeding (*surveillance, inspect, intrude*) en aanvallende capaciteiten inzetten (*disrupt, degrade, disconnect, discomfort, distrust*) wanneer dat noodzakelijk is. Wat een tegenstander kan, kunnen wij immers ook en mogelijk zelfs beter. Defensie moet samen met andere relevante organisaties nieuwe bijbehorende juridische en ethische raamwerken mee helpen ontwikkelen om niet te ontsporen, maar wel effectief te kunnen zijn. Er bestaan overigens al juridische mogelijkheden om sociale media in Nederlandse militaire operaties in te zetten. De interpretatie hiervan behoeft een ethische en politieke discussie.[28]

28 Zie: Gortworst, *Sociale media als wapen*.

Ten tweede moet het besef doordringen dat alles en iedereen een rol heeft in het informatiedomein, dus ook de traditionele militaire (gevechts)eenheden. Elke (gevechts)actie creëert immers een beeld, en daarmee ook een verplaatsing of militair geweld, wat moet passen in de te bereiken perceptiedoelstellingen. Dit betekent dat elk fysiek en niet-fysiek militair handelen moet passen in onze overkoepelende informatiedoelstelling. Militair handelen zonder informatiebelang is zinloos en mogelijk zelfs contraproductief en zou eigenlijk niet meer mogen voorkomen.

Sommige specialistische eenheden, zoals cyber-, EOV-, of communicatie-eenheden hebben een speciale rol in het informatiedomein. Deze specialistische eenheden kunnen, als derde maatregel, samengevoegd worden tot CEMA-eenheden of Information Manoeuvre Force-eenheden. Deze rol is niet langer ondersteunend, maar bepalend geworden: de nieuwe speerpunt van de zwaardmacht zijn Information Manoeuvre Force-eenheden. Maar *al* het optreden heeft effect in het informatiedomein. Er moet daarom gesynchroniseerd optreden zijn in alle domeinen en dimensies om informatiedoelstellingen te bereiken en de War on Perception te winnen of om in ieder geval stand te kunnen houden.

Als vierde moet Defensie prioriteit geven aan CEMA-eenheden. CEMA is de combinatie van analoge en digitale EOV, tactische SIGINT en tactische Cyber. Tactische SIGINT en cyber betekent het aanvallen en verdedigen van tactische doelen, bijvoorbeeld gesegmenteerde netwerken met eenvoudige encryptie die gebruikt wordt op de lagere uitvoerende echelons.
Hiertoe moet Defensie (civiele) specialisten aantrekken, militair CEMA-personeel behouden, versnelde en vergrote materieelprojecten uitvoeren, experimenteren, specialistische oefeningen opzetten, *distributed* EOV invoeren, alle grotere wapenplatforms uitrusten met sensoren en *jammers*, de internationale samenwerking op CEMA-gebied intensiveren, wetenschappelijk onderzoek op dit gebied uitbreiden, doctrine moderniseren, sneller nieuwe materieel en surveillance-, jamming-, analyse-, encryptie- en decodeer-software invoeren en vooral CEMA-specialisten in hun kracht zetten. Doet Defensie dit niet dan zijn we niet alleen krachteloos, maar ook weerloos.

Op het digitale battlefield of information warfare moet Defensie militair vermogen anders organiseren, meer gericht op het werkelijke zwaartepunt van toekomstige oorlog: vertrouwen

Als vijfde maatregel moet Defensie niet alleen de Nederlandse staat en bevolking, maar ook de strijdkrachten verdedigen tegen vijandelijke Information Manoeuvre-activiteiten. Dit betekent dat zowel ons eigen vermogen tot informatie-handelen (systemen) als onze verbindingen (netwerken) en onze menselijke geesten (minds) moeten worden beschermd. Desinformatie moet worden geïdentificeerd en bestreden en achterliggende duistere organisaties onthuld.[29] Ook de data en informatie zelf moet worden beschermd tegen malversaties.
Als zesde moet Defensie ook snel aan de slag gaan met het opstellen van Information Manoeuvre-doctrine en operationele processen. Information Manoeuvre-opleidingen moeten worden ontwikkeld en opgezet. Tevens moet Information Manoeuvre een veel centralere rol krijgen in militaire stafprocessen, niet alleen op het tactische niveau, maar ook op het operationele, militair strategische en zelfs civiel-militair-strategische niveau. Het prestige van Information Manoeuvre-specialisten moet omhoog; ze zijn niet langer adviseurs, maar Information Manoeuvre-strijders, met de (digitale) sleutels tot de overwinning in hun handen.

Daarnaast moeten – als laatste – ook de traditionele gevechts-, gevechtsondersteunende

29 Sommige bedrijven zijn hierin gespecialiseerd, zoals Debunk Incorporated.

Sommige specialistische eenheden, zoals EOV, hebben een rol die niet ondersteunend, maar bepalend is in Information Manoeuvre

en gevechtslogistieke eenheden rekening houden met de gevolgen van Information Manoeuvre. Hierbij valt te denken aan grotere spreiding van commandoposten, meervoudige verbindingen, betere encryptie van de connecties, andere vormen van databasebeheer, betere doctrine, betere opleidingen en het inpassen van civiele experts. Maar ook het verminderen van de 'verticale afhankelijkheid' is hierbij belangrijk. Horizontale, zelforganiserende bewapende netwerken zijn immers de organisatievorm van de toekomst, omdat ze sneller, flexibeler, minder kwetsbaar en adaptiever zijn en beter kunnen samenwerken met de vele andere actoren die het (online)slagveld inmiddels hebben betreden: de *Power to the Edge* en *NetForce* gedachte.

Afsluiting

Veranderende informatietechnologie heeft gevolgen voor de machtsordening, terwijl die technologie zelf disruptieve kenmerken vertoont. Om in het informatiedomein te kunnen manoeuvreren zijn veranderingen in de defensieorganisatie nodig, waar ik hierboven voorstellen voor gedaan heb. De veranderingen

FOTO MCD, KEESNAN DOGGER

zijn noodzakelijk, omdat de krijgsmacht anders binnenkort niet meer relevant zal zijn. Informatie is immers het wapen van de toekomst.

Uiteindelijk draait het om zes belangrijke aandachtspunten:

- *Informatie is het wapen van de toekomst.* Verhalen, beelden en percepties zijn belangrijker dan schepen, vliegtuigen en kanonnen. Alles draait om de *Battle of the Narrative.* Kracht zit niet langer in fysieke vernietigingseffecten, maar in het vermogen om het discours van een conflict te beïnvloeden, zowel aan eigen zijde als aan vijandelijke en neutrale kant. Het gaat niet langer om wiens leger fysiek wint, maar om wiens verhaallijn wint;
- *Informatie Manoeuvre is altijd live.* Information Manoeuvre moet worden uitgevoerd voor, tijdens en na een conflict. Het stopt nooit. We zijn in permanente staat van (digitale) oorlog. Informatietechnologie ontwikkelt zich bovendien razendsnel en daarom is het een continue wedloop van 'studeren, experimenteren, implementeren, beschermen en aanpassen';
- *Information Manoeuvre kent geen veilige gebieden en geen non-combattanten.* Alles en iedereen is een doelwit, van de eigen strijdkrachten en vijandelijke strijdkrachten tot neutrale partijen en de eigen bevolking. Van grijsaard tot kind. Er zijn geen veilige gebieden meer;
- *Information Manoeuvre moet gericht zijn op zowel informatie-handelingscapaciteit als beïnvloeding van de menselijke geest*. Val geen gevechtskracht aan, maar val commandoposten, netwerken, databases en 'vertrouwen' aan;
- De nieuwe digitale vijandelijke online strijders moeten aangevallen worden met *nieuwe digitale civiele technieken.* Die technieken moeten we uit de civiele wereld halen en aanhechten aan onze militaire bewapende netwerken. Bevecht Homo Digitalis met Militia Digitalis;
- *Watch the dark side of information.* Heb aandacht voor de duistere kant en corrumperende werking van informatie, anders hebben we geen vijand nodig om ons te verslaan.

Op het digitale battlefield of information warfare zijn nieuwe wapens nodig. Sociale media zijn geen vijand, maar bieden ongekende mogelijkheden voor het beïnvloeden van een grote diversiteit aan doelgroepen om missiedoelstellingen naderbij te brengen en het eigen militaire vermogen en de (rechts)staat te beschermen. De spelregels van oorlogvoering veranderen en informatie wordt het wapen van de toekomst. Het is daarom hoog tijd dat Defensie dit inziet en militair vermogen anders organiseert, meer gericht op het werkelijke zwaartepunt van toekomstige oorlog: vertrouwen. Information Manoeuvre is de hierbij behorende gevechtsvorm, informatie het meest geëigende wapen en 'waarheid' is de munitie. ■

Zeg me dat het niet waar is…?

Nederlands beleid en de rol van de krijgsmacht tegen desinformatie

Door sociale media kan nieuws zeer snel worden doorgegeven. Maar wat als dat nieuws desinformatie bevat, waarmee kwaadwillenden uit zijn op misleiding of zelfs destabilisatie? In Nederland is de minister van Binnenlandse Zaken en Koninkrijksrelaties de kartrekker bij het formuleren van beleid voor het tegengaan van desinformatie. Ook voor Defensie is er een rol weggelegd. Militairen moeten voorbereid zijn op blootstelling aan desinformatie en op de Nederlandse Defensie Academie worden daar al lessen over gegeven. Volgens deskundigen moet er, om effectief op desinformatie te kunnen reageren, een betere integratie plaatsvinden tussen het fysieke domein en de informatieomgeving en dient Defensie de eigen strategische communicatie goed op orde te hebben. Tevens moet de Defensiestaf nu al nadenken hoe een eventueel verzoek van de regering om militaire capaciteit in te zetten tegen desinformatie ingewilligd zou kunnen worden.

Tweede-luitenant Bo van den Herik, dr. Tine Molendijk en kolonel Han Bouwmeester[*]

'Zeg me dat het niet zo is, … zeg me dat het niet waar is', zong Frank Boeijen over een bekende van hem die ongeneeslijk ziek was.[1] Dat was in 1989, meer dan dertig jaar geleden. Anders dan bij Frank Boeijen, die de aankomende dood van een dierbare liever niet onder ogen wilde zien, willen veel mensen tegenwoordig bepaalde informatie niet meer tot zich nemen, puur omdat ze deze niet vertrouwen. Door de communicatierevolutie van internet en mobiele telefonie is de top-down informatieverspreiding gekanteld van 'hoog naar laag' naar 'van één naar velen'. Hierdoor is een horizontale informatieverspreiding ontstaan waarbij iedereen als zender op kan treden.[2] Dit verschijnsel heet *citizen journalism,* burgerjournalistiek, waarbij mensen die vroeger het publiek vormden, nu zelf mediamiddelen hebben om elkaar te informeren. Ze zijn daarbij niet gebonden aan codes die gelden voor kwaliteitsjournalistiek.[3] Ondanks deze mogelijkheden zijn veel mensen tegenwoordig ontevreden over de nieuwsvoorzieningen. Er is niet alleen kritiek op sociale media, ook de *mainstream* media, de kranten, radio en televisie, moeten het vaak ontgelden, vooral als ze met nieuws komen dat strijdig is met de bestaande mening van de nieuwsconsument. Deze consument dient vooral ook kritisch naar zichzelf te kijken, want hij blijft verantwoordelijk voor zijn eigen nieuwsgaring. Een nieuwsconsument kan de laatste jaren steeds sneller en meer nieuws tot zich nemen, ook nieuws waarbij geen *fact-checking* en hoor-en-wederhoor heeft plaatsgevonden. Er lijkt een *overload* aan oncontroleerbare informatie te ontstaan waarbij het gros van de nieuwsconsumenten alleen nog die informatie accepteert die de eigen mening sterkt. Feitelijkheden doen er minder toe. Slechts weinigen verzuchten: 'Klopt dit wel? Welke informatie kan ik nog vertrouwen?' Het roept ook de vraag op of de absolute waarheid eigenlijk wel bestaat.

Over het ontstaan en de aanpak van het coronavirus doen veel verhalen de ronde, waardoor er al snel een situatie van information disorder heerste

FOTO MCD, JASPER VEROLME

De Raad van Europa,[4] die ook onderzoek doet naar gemanipuleerde informatie, spreekt bij zo'n onzekere situatie het liefst over *information disorder*, een toestand waarin veel emotionele en oncontroleerbare informatie aanwezig is. Het is daarbij lastig de bron, de *digital patient zero*, te achterhalen, en niemand weet dan hoe betrouwbaar de informatie is. Vaak komt de informatie in eerste instantie geloofwaardig over en dat maakt het nog lastiger om de informatie geheel te negeren.[5] Enkele recente voorbeelden van information disorder zijn de diverse verhalen over de oorzaak van de MH17-ramp en de verhalen over het ontstaan en de aanpak van het Covid-19-virus. Het lijkt er sterk op dat er, zodra zich nieuws aandient over mensen en incidenten, een spook van desinformatie rondwaart door de wereld.

Ook de Nederlandse samenleving blijft niet gespaard. Aangezien dit themanummer van de *Militaire Spectator* zich richt op beïnvloeden met informatie mag een artikel over wat de Nederlandse overheid – inclusief de krijgsmacht – doet tegen desinformatie niet ontbreken. Het is immers een van de kerntaken van de overheid om de interne en externe veiligheid van de Nederlandse samenleving onder alle omstandigheden te waarborgen.[6] De centrale vraag in dit

* Dit artikel is een bewerking van de in het voorjaar van 2020 geschreven afstudeerscriptie van tweede-luitenant Bo van den Herik voor zijn studie Militaire Bedrijfswetenschappen aan de Nederlandse Defensie Academie (NLDA). Hij werd begeleid door dr. Tine Molendijk, docent bij de vakgroep Militaire Bedrijfswetenschappen, en kolonel Han Bouwmeester, docent bij de vakgroep Krijgswetenschappen, die beiden een bijdrage hebben geleverd aan de totstandkoming van dit artikel.

1 'Het Verhaal achter 'Zeg me dat het niet zo is' van de Frank Boeijen Groep', *NPO Radio 2* (16 december 2018). Zie: https://www.nporadio2.nl/nieuws/24295/het-verhaal-achter-zeg-me-dat-het-niet-zo-is-van-frank-boeijen-groep.

2 H. Beunders, 'Crisis der Zekerheden', in: *Christen Democratische Verkenningen* (Lente 2018) 113.

3 J. Rosen, 'A Most Useful Definition of Citizen Journalism', *PressThink Website* (14 juli 2008). Zie: http://archive.pressthink.org/2008/07/14/a_most_useful_d.html.

4 De Raad van Europa omvat alle regeringsleiders uit Europa en de Kaukasus, met uitzondering van Kazachstan, Wit-Rusland en Vaticaanstad en is gericht op het bevorderen van eenheid tussen de lidstaten, veiligheid en het borgen van mensenrechten.

5 C. Wardle en H. Derekhshan, *Information Disorder. Toward an Interdisciplinary Framework for Research and Policy Making*, 2nd Revised Edition, Council of Europe Report, (Straatsburg, Raad van Europa, 2018) 12-13.

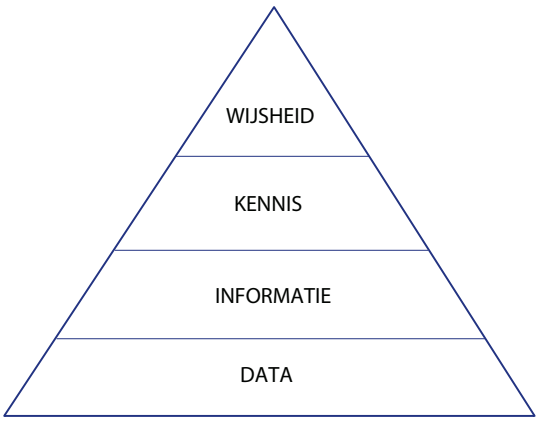
6 P. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding* (dissertatie Universiteit van Amsterdam) (Nijmegen, Wolf Legal Publishers, 2008) 12.

artikel is dan ook hoe de Nederlandse overheid en krijgsmacht omgaan met desinformatie. Om deze vraag te beantwoorden gaat dit artikel allereerst in op het begrip desinformatie. Wat is het? En is desinformatie een universeel begrip? Daarna komen de maatregelen die de Nederlandse overheid heeft genomen om desinformatie te bestrijden aan de orde en de rol die de krijgsmacht daarbij speelt. Ten slotte volgen een conclusie en een waarschuwing.

Desinformatie

Wat is desinformatie eigenlijk? En wat doet het met een mens? Al in 1949 onderkenden de wiskundige Claude Shannon, gezien als de grondlegger van de informatietheorie, en zijn rechterhand Warren Weaver dat informatie een essentieel deel is van een lineaire communicatieketen waarbij sprake is van eenrichtingsverkeer. Een zender pikt informatie op uit zijn omgeving en zet die om in een boodschap, die via een bepaald kanaal uiteindelijk bij een ontvanger terecht komt. De ontvanger wordt vervolgens in meer of mindere mate beïnvloed door deze boodschap. Shannon en Weaver stelden vast dat er onderweg in de keten ruis zou kunnen optreden, wat de informatie kan vervormen. Zij wilden ook weten of er een verschil meetbaar was tussen de verzonden informatie en de ontvangen informatie, en wat de ontvanger er vervolgens mee deed. Zij zagen als één van de eersten in dat informatie een beïnvloedende werking heeft.[7]

Het onderzoek van Shannon en Weaver was een inspiratie voor vele anderen en snel begon de communicatiewetenschap zich te ontwikkelen. In 1962 deden gedragswetenschappers in de Verenigde Staten een aantal experimenten om te kijken hoe mensen bepaalde vormen van ruis in communicatie konden onderkennen. Ze bekeken ook hoe een boodschap uiteindelijk een *state of mind* bij mensen kon oproepen.[8] In 1976 publiceerden de Amerikaanse communicatiewetenschapper Nicholas Belkin en de Britse informaticus Stephen Robertson een baanbrekend artikel, waarin ze stelden dat informatie datgene is dat bepaalde denkstructuren bij een mens kan veranderen. Mensen zijn niet alleen in staat met informatie een beeld van zichzelf en hun omgeving op te bouwen, maar kunnen met nieuwe informatie dit beeld ook aanpassen. Zo ontstaan percepties.[9] Tien jaar later verklaarden onderzoekers dat informatie datgene is wat het menselijke brein constant creëert om betekenis te geven aan waarnemingen uit de omgeving; het is niet iets wat al bestaat.[10]



Figuur 1 De cognitieve of DIKW-hiërarchie van Ackoff

Een stap verder in de beschouwing van informatie is hoe de mens bepaalde informatie verwerkt, en dat valt uit te leggen via de cognitieve of DIKW-hiërarchie van Ackoff. Russell Ackoff, een Amerikaanse organisatiedeskundige, brengt in zijn cognitieve hiërarchie vier niveaus aan: Data, Informatie, Kennis en Wijsheid. Ackoff beschouwde *data* als iets wat los staat van enige vorm van menselijke verwerking en daarmee nog vrij is van interpretatie. Het is een verzameling van feiten in een ruwe, ongeorganiseerde vorm. Een mens kent waarde toe aan data door onderliggende verbanden te onderkennen en zo ontstaat een samenhangend geheel dat informatie wordt genoemd. *Informatie*

7 D. McQuail en S. Windahl, *Communication Models. For the Study of Mass Communication*, 2nd Edition, (Harlow, Addison Wesley Longman Limited, 1996) 16-17.

8 R. Taylor, 'The Process of Asking Questions', in: *American Documentation*, 13 (1962) 4, 391-396.

9 N. Belkin en S. Robertson, 'Information Science and the Phenomenon of Information', in: *Journal of the American Society for Information Science*, 27 (1976) 4, 198-199.

10 B. Dervin en M. Nilan, 'Information Needs and Uses', in: *Annual Review of Information Science and Technology (ARIST)*, 21 (1986) 20-22.

is gemakkelijker te visualiseren en te analyseren. Zodra een persoon ook patronen in de informatie kan herkennen en informatie kan categoriseren ontstaat kennis. Bij *kennis* is er sprake van relevantie van de informatie; het verband tussen data krijgt op dit niveau betekenis. Een mens gaat zo relaties leggen met andere delen van informatie, die onder meer is verkregen uit eerdere ervaringen. Er kan uiteindelijk *wijsheid* ontstaan bij een mens als die zich gaat afvragen waarom bepaalde zaken zijn zoals ze zijn en de daarbij ontstane kennis in perspectief weet te plaatsen. Een mens weet dan onderliggende principes te doorgronden en verschijnselen in zijn omgeving nader te verklaren.[11]

Er is ook kritiek op de cognitieve hiërarchie van Ackoff. Een van de bekendste critici is Jay Bernstein, een bekende Amerikaanse filosoof, die terecht aangaf dat Ackoff zich alleen maar toelegde op de verwerking van alleen die informatie, die ook tot wijsheid kan leiden. Bernstein benaderde de cognitieve hiërarchie daarom van bovenaf en ging uit van tegenpolen van wijsheid-kennis-informatie-data. Tegenover wijsheid stelde Bernstein *stupidity*, onbenulligheid, die volgens hem voortkwam uit *ignorance*, onwetendheid of wellicht ongeïnteresseerdheid. De ignorance was het gevolg van desinformatie en misinformatie, als tegenpool van informatie. Een tegenpool voor data bestaat niet, er is niet zoiets als anti-data. Bernstein wilde laten zien dat er bij een mens, als hij wordt gevoed met gemanipuleerde informatie, andere percepties ontstaan.[12] Het is een fascinerende, maar tegelijkertijd ook beangstigende constatering dat een mens zo gemakkelijk en ongemerkt kan worden beïnvloed.

Desinformatie en misinformatie worden vaak in één adem genoemd, maar er is een verschil. Misinformatie is verkeerde of onnauwkeurige informatie die wordt gedeeld, maar niet noodzakelijkerwijs om iemand te misleiden. Desinformatie, daarentegen, is het opzettelijk verspreiden van verkeerde informatie met de bedoeling om iemand te misleiden.[13] De Raad van Europa hanteert nog een derde categorie verkeerd gebruikte informatie, de zogeheten malinformatie. Malinformatie is gebaseerd op de werkelijkheid, maar roept boze reacties op. Kwaadwillende mensen of groepen verspreiden deze malinformatie opzettelijk om personen, organisaties of landen te beschadigen. De gebruikers weten bepaalde aspecten van de werkelijkheid, bijvoorbeeld een slechte eigenschap van iemand, uit te vergroten om zodoende kwaad over iemand te spreken, zoals bij smaad en haatpreken.[14] Ook bepaalde vormen van propaganda, waarbij heel nadrukkelijk het wij-zij-gevoel wordt opgeroepen, behoren tot malinformatie.[15]

De verspreiding van desinformatie beslaat drie elementen, vergelijkbaar met een lineair en

FOTO RAAD VAN EUROPA, ELLEN WUIBAUX

De Britse journalist David Patrikarakos spreekt op een bijeenkomst van de Raad van Europa over desinformatie en zijn boek War in 140 Characters. How Social Media is Reshaping Conflict in the Twenty-First Century

11 R. Ackoff, 'From Data to Wisdom', in: *Journal of Applied System Analysis*, 16 (1989) 1, 3-9.
12 J. Bernstein, 'The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis', in: E. Jacobs en B. Kwasnik, *Proceedings North American Symposium on Knowledge Organization*, Volume 2 (Syracuse, Academic Press, 2009) 68-75.
13 J. Fetzer, 'Disinformation: The Use of False Information', in: *Minds and Machines*, 14 (2004) 231-232. M. Tudjman en N. Mikelic, *Information Science: Science about Information, Misinformation and Disinformation*, Conference Paper (Zagreb, Universiteit van Zagreb, 2003); D. Fallis, 'Mis- and dis-information', in: L. Floridi, *The Routledge Handbook of Philosophy of Information* (Abingdon, Routledge, 2016) 332-344.
14 Wadle en Derekhshan, *Information Disorder*, 20-22.
15 H. Lasswell, *Propaganda Technique in the World War* (oorspronkelijk uitgegeven in 1927) (New York, Peter Smith Publishers, 1938) 195-196.

eenzijdig gericht communicatiemodel: de verspreider, de boodschap en de ontvanger. De verspreider kan verschillend zijn samengesteld, individueel of in groepsverband, en diverse karakteristieken hebben. Over het algemeen streven de meeste verspreiders een van de volgende drie motieven na:

- financieel: eraan verdienen;
- politiek: een bepaalde kandidaat in diskrediet brengen om zelf te profiteren;
- sociaal-psychologisch: bij een groep willen horen en aanzien krijgen.[16]

De inhoud van de boodschap kan sterk variëren, maar waar een ontvanger vooral op moet letten is hoe zorgvuldig een boodschap is samengesteld en of een boodschap onwettige of bedrieglijke elementen bevat. Onderzoek heeft uitgewezen dat er vier karakteristieken zijn die een boodschap aantrekkelijk maken en de kans vergroten dat de ontvanger de boodschap accepteert:

- een prikkelende inhoud om een emotionele reactie op te wekken;
- een sterke visuele component omdat veel mensen visueel zijn ingesteld;
- een sterk narratief om richting te geven en om het eventueel naast een ander sterk verhaal te plaatsen;
- herhaling van de boodschap, zodat deze blijft kleven in de gedachten van de mens.[17]

Bij de ontvanger spelen, naast de eigen informatieverwerkingsprocessen, ook de reacties op desinformatie een rol.[18] Zo is er een tendens dat radicale individuen en groepen zich vooral bezighouden met 'guerrilla desinformatie', gericht tegen een bepaalde regering of organisatie. Met behulp van zogeheten *false news planters* willen deze radicalen sociale chaos opwekken door middel van opruiende berichten op het internet – ook wel *cyber hooliganism* genoemd – om daarmee eigen belangen op de agenda te krijgen of te realiseren. Landen die desinformatie inzetten willen andere regeringen ondermijnen, samenlevingen ontwrichten en verdeeldheid kweken en de nationale veiligheid van andere staten aantasten om zelf een sterkere internationale positie te verkrijgen.[19]

Een universeel begrip?

Politieke leiders beschuldigen hun opponenten in de wereld graag van het verspreiden van desinformatie. Een effectieve bestrijding van desinformatie dient zich daarom ook te richten op de vraag of volkeren en landen desinformatie allemaal hetzelfde definiëren. Deze vraag is actueel omdat het probleem van desinformatie geen nationaal probleem is; het overschrijdt gemakkelijk de landsgrenzen.

Is er overal wel een scherpe tweedeling in 'zuivere' informatie en desinformatie? Het lijkt misschien vanzelfsprekend dat er een strikte scheiding mogelijk is tussen objectiviteit en subjectiviteit, beschrijving en opinie, en feit en fictie, maar dat geldt niet overal.[20] Neem bijvoorbeeld de beruchte desinformatiecampagnes van de Sovjet-Unie. De autoriteiten verspreidden hier actief onwaarheden en zagen dit vooral als een manier om 'grotere waarheden' over de aard van het kapitalisme bloot te leggen.[21] Daarnaast is het zo dat er in veel landen juist wantrouwen heerst tegenover de informatie vanuit de eigen gevestigde orde. Ook is er niet overal veel vertrouwen dat journalistiek onafhankelijk is van de staat.[22] Dit leidt er toe dat het geloof in de beschikbaarheid van strikt objectieve kennis in veel landen minder groot is dan in bijvoorbeeld Nederland, of zelfs helemaal niet bestaat.

16 Wardle en Derekhshan, *Information Disorder*, 22-39.
17 Ibidem.
18 Ibidem.
19 J. Bugajski, 'The Geopolitics of Disinformation', zie: Center for European Policy Analysis (CEPA): http://infowar.cepa.org/The-geopolitics-of-disinformation.
20 C. Scott, 'Science for the West, Myth for the Rest', in: L. Nader (red.), *Naked Science. Anthropological Inquiry into Boundaries, Power, and Knowledge* (New York, Routledge, 1996) 69-86; M. Haigh, T. Haigh en N. Kozak, 'Stopping Fake News. The Work Practices of Peer-to-Peer Counter Propaganda', in: *Journalism Studies*, 19 (2018) 14, 2062-2087; T. Hanitzsch, 'Journalism Studies Still Needs to Fix Western Bias', in: *Journalism*, 20 (2019) 1, 214-217.
21 I. Pacepa en R. Rychlak, *Disinformation. Former Spy Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism* (Washington, D.C., WND Books, 2013) 35-43.
22 Hanitzsch, 'Journalism Studies Still Needs to Fix Western Bias', 214-217; E. Humprecht, 'Why Resilience to Online Disinformation Varies Between Countries', in: *Media@LSE* (8 april 2020). Zie: https://blogs.lse.ac.uk/medialse/2020/04/08/why-resilience-to-online-disinformation-varies-between-countries.

Dit verschil tussen landen wil niet zeggen dat mensen elders helemaal geen onderscheid tussen werkelijkheid en propaganda maken, maar wel dat zij minder snel kiezen voor bepaalde oplossingen. Vooral in Noord-Amerika en in Europese landen zijn bewustwordingscampagnes en fact-checking-acties geïnitieerd, maatregelen waarin het idee van objectiviteit duidelijk resoneert.[23] Daarnaast zijn er verschillen in interpretatie van wat objectiviteit precies inhoudt. Waar het in sommige landen bijvoorbeeld haast een harde voorwaarde is dat maatregelen tegen desinformatie zo a-politiek mogelijk zijn, verbinden initiatiefnemers in andere landen hun activiteiten juist vaak expliciet aan een politieke boodschap.[24] In sommige landen heerst namelijk de opvatting dat mensen informatie alleen maar als feitelijk aannemen als deze vrij is of vrij lijkt te zijn van ideologie, terwijl elders het omgekeerde eerder het geval is.

Tegelijkertijd is mondiaal een tendens waarneembaar van toenemende twijfel over het idee van objectiviteit. Mensen zijn zich er bewuster van geworden dat propaganda ook in de eigen regio bestaat, al dan niet in de vorm van *alternative facts* of *fake news*, of in ieder geval dat vooringenomenheid deels onvermijdelijk is.[25] Dit maakt de bestrijding van desinformatie moeilijker, want in plaats van kritischer kan het mensen ook juist ontvankelijker maken voor desinformatie. Tevens lijkt het te zorgen voor een groeiend besef dat desinformatie niet alleen bestreden moet worden met ontmaskeringstrategieën zoals fact-checking, maar ook met het actief creëren van overtuigende (tegen)verhalen.[26] Culturele verschillen in opvattingen over wat desinformatie is spelen in ieder geval een duidelijke rol in de maatregelen die landen ertegen nemen en – nog belangrijker – bij de effectiviteit ervan.

De Nederlandse overheid

De Nederlandse samenleving is een open maatschappij, die veelvuldig getroffen wordt door allerlei vormen van desinformatie. Deze paragraaf gaat in op de maatregelen die de Nederlandse overheid heeft genomen. Hiertoe zijn beleidsdocumenten van betrokken overheidsorganisaties bestudeerd en zijn interviews gehouden met experts van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Defensie, het Commando Landstrijdkrachten, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Rathenau Instituut.[27]

Nederland heeft de aanpak van desinformatie belegd bij de minister van BZK. Op 13 november 2017 maakte de minister van BZK voor het eerst gewag van desinformatie. Desinformatie, zo schrijft de minister in een Kamerbrief, is samen met selectieve informatie een vorm van politieke beïnvloeding en een brede verspreiding daarvan kan 'makkelijk, anoniem, snel en goedkoop.'[28] De minister geeft aanvankelijk verder geen uitleg over desinformatie. De correspondentie tussen de minister en de Tweede Kamer blijft in die tijd beperkt tot het alert zijn op de verspreiding van desinformatie in Nederland. Eind februari 2018 stelt de minister dat desinformatie te onderscheiden is van foutieve berichtgeving in het algemeen. Bij desinformatie beseft de originele afzender dat het gaat om foutieve informatie, bovendien heeft hij de intentie om hiermee anderen te misleiden, aldus de minister.[29]

Tegenwoordig hanteert de minister van BZK wel degelijk een definitie: 'Desinformatie is het doelbewust, veelal heimelijk, verspreiden van

23 D. Funke en D. Flamini, 'A Guide to Anti-Misinformation Actions Around the World', in: *Poynter*, 9 april 2018.

24 L. Graves, 'Boundaries Not Drawn', in: *Journalism Studies*, 19 (2016) 5, 613–631.

25 J. Bogaerts en N. Carpentier, 'The Postmodern Challenge to Journalism. Strategies for Constructing a Trustworthy Identity', in: C. Peters en M.J. Broersma (red.), *Rethinking Journalism* (New York, Routledge, 2013) 72-84.

26 M. Levinger, 'Master Narratives of Disinformation Campaigns', in: *Journal of International Affairs*, 71 (2018) 1.5, 125-134

27 Het Rathenau Instituut is een onafhankelijke organisatie die zich bezighoudt met kwesties waarbij wetenschap, technologie en samenleving elkaar overlappen. Het instituut valt onder de Koninklijke Nederlandse Akademie van Wetenschappen en is gevestigd in Den Haag.

28 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief over Beïnvloeding van de Publieke Opinie door Statelijke Actoren*, Kenmerk 8df6065b-or1-4.0, dd. 13 november 2017.

29 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Beantwoording Kamervragen over desinformatie en beïnvloeding door Statelijke Actoren*, Kenmerk 2018-0000145443, dd. 28 februari 2018.

FOTO RIJKSOVERHEID, HENRIËTTE GUEST

De bestrijding van desinformatie is belegd bij het ministerie van BZK, waarbij de effecten van de digitalisering op de democratie de aandacht hebben

misleidende informatie, met als doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid. […] Desinformatie hoeft niet altijd onjuiste informatie te bevatten. Het kan een combinatie zijn van feitelijke, onjuiste en deels onjuiste informatie, maar altijd met de intentie om te misleiden en te schaden.'[30]

De geïnterviewde experts kunnen zich over het algemeen vinden in de definitie van de minister. Een van de experts voegde nog toe dat het uiteindelijke doel van desinformatie is om percepties of handelen van mensen en organisaties te beïnvloeden. Een andere expert merkte op dat Nederland wel sterk verschilt van andere landen die geen 'polder-consensus-overleg'-structuur hebben. Het verschilt in Nederland per betrokken ministerie hoe er over desinformatie wordt gesproken. En waar het ene ministerie aangeeft een wet te willen ontwerpen voor het tegengaan van desinformatie, stelt het andere ministerie dat dit niet nodig is.

Hoewel de experts aangeven dat ze kunnen instemmen met de definitie van de minister, is het opvallend dat de betrokken departementen elkaar op twee essentiële aspecten betwisten, namelijk wat desinformatie precies is en hoe het bestreden moet worden. Ambtenaren van elk betrokken ministerie willen dat hun belangen worden meegenomen in de bestrijding van desinformatie, ook al staan deze haaks op het beleid van een ander ministerie. Voormalig hoogleraar bestuurskunde en oud-minister Uri Rosenthal noemde een dergelijke stammenstrijd een vorm van *bureaupolitisme*. Hij zegt dat een situatie van bureaupolitiek, met verschillende ambtelijke actoren en verschillende belangen, te ver kan doorschieten, waarbij de belangenconcurrentie verlammend gaat werken en waardoor ondoelmatigheid en desintegratie kunnen ontstaan.[31] Hier schuilt een gevaar voor de interdepartementale aanpak van desinformatie.

30 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief over Beleidsinzet Bescherming Democratie tegen Desinformatie*, Kenmerk 2019-0000546545, dd. 18 oktober 2019.

31 U. Rosenthal, *Bureaupolitiek en Bureaupolitisme. Om het Behoud van een Competitief Overheidsbestel* (bewerking van een oratie) (Alphen a/d Rijn, Wolters Kluwer, 1988).

Een adequate aanpak is geboden, want volgens Kamerbrieven heeft de Nederlandse samenleving veelvuldig last van Russische beïnvloedingsactiviteiten op sociale media, onder meer over de toedracht van de ramp met de MH17.[32] In mei 2020 schreef de minister van BZK dat op dat moment veel misleidende informatie rondging over Covid-19. Het ging vooral om veel misleidende informatie over de oorzaak van het coronavirus en over maatregelen die de Nederlandse overheid neemt.[33]

Effectieve beleidsmaatregelen van de overheid, niet anders dan het desinformatiebewustzijn van burgers en politici te stimuleren en de bevordering van mediawijsheid, zijn nog summier benoemd. Daarom ligt het voor de hand om uit de gehouden interviews met de experts een viertal thema's, die de Nederlandse overheid probeert in te zetten, verder uit te diepen: bewustwording, sociale media, het versterken van de informatiepositie, en de reactie op desinformatie.

Bewustwording

Het vergroten van de maatschappelijke weerbaarheid kan een rol spelen in het tegengaan van desinformatie.[34] De samenleving moet dan wel onderkennen dat er een dreiging is. Zo laat onderzoek naar het weerstandsvermogen van mensen zien dat personen die zich in zekere mate bewust zijn dat ze constant worden bestookt met beïnvloedende informatie, minder snel zijn te manipuleren.[35] Uit de interviews met experts kwam het belang van bewustwording sterk naar voren om de Nederlandse samenleving weerbaarder te maken tegen desinformatie. Zo heeft ook de NCTV veel tijd gestopt in overleg met gemeenten om het bewustzijn te vergroten.

De overheid zet ook in op individuele bewustwording en wil maatregelen ter stimulering van mediawijsheid. Hiervoor zijn diverse campagnes gestart en wordt in het curriculum voor het primair en voortgezet onderwijs het thema mediawijsheid opgenomen als onderdeel van digitale vaardigheden.[36] Dit zou moeten helpen bij het weerbaarder maken van de Nederlandse burger tegen desinformatie. Zoals één van de experts stelde: 'Je wilt zorgen dat de Nederlandse burger weerbaar is en niet zomaar alles gelooft wat er online voorbijkomt.' Een onderzoek van I&O Research, uitgevoerd in opdracht van *de Volkskrant*, laat zien dat slechts 29 procent van de in totaal 2434 respondenten aangeeft in staat te zijn om feitelijk van nep-nieuws te onderscheiden. Daarbij valt op dat 39 procent van de online-verzamelaars zegt het onderscheid tussen echt nieuws en nepnieuws te maken, terwijl de mainstream-mediaconsumenten slechts op 24 procent uitkomen.[37] Kortom, er is nog een aanzienlijke weg te gaan om de Nederlandse bevolking kritischer naar informatie te leren kijken.

Sociale media

De Nederlandse samenleving kent een grote pluriformiteit aan nieuwsvoorziening.[38] Zo stelt één van de experts dat Nederland een 'uitgebreide mediamenukaart' kent. Mensen halen hun nieuws uit verschillende bronnen. Veel nieuwsmedia zitten tegenwoordig ook op sociale media, waarbij mensen kunnen reageren op online-artikelen. Deze aspecten verkleinen de kans dat mensen veelvuldig en eenzijdig desinformatie tot zich nemen en accepteren. Aan de andere kant betekent het toenemende belang van het internet wel dat desinformatie zich gemakkelijker kan verspreiden, waarbij citizen journalism een rol speelt; burgers zonder enige journalistieke achtergrond hebben de mogelijkheid nieuws te creëren en te ver-

32 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief,* met kenmerk 2019-0000546545.

33 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief Ontwikkelingen Beleidsinzet Bescherming Democratie tegen Desinformatie,* Kenmerk 2020-0000245897, dd. 13 mei 2020.

34 C. Versteegden, *Resilience Can Counter Dezinformatsiya. How the Military Considers its Contribution to Enhancing Dutch Resilience* (Master Thesis for the Military Strategic Studies Programme) (Breda, Faculteit Militaire Wetenschappen NLDA, 2018) 19.

35 J. Quinn en W. Wood, 'Forewarnings of Influence Appeals. Inducing Resistance and Acceptance', in: E. Knowles en J. Linn (red.), *Resistance and Persuasion* (Mahwah, Lawrence Erlbaum Associates Publishers, 2004) 200.

36 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief,* met kenmerk 2019-0000546545.

37 P. Kanne en M. Driessen, *Desinformatie leidt tot verwarring bij de nieuwsconsument,* Onderzoeksrapport voor *de Volkskrant* (Amsterdam, I&O Research, 2017) 27-29.

38 M. de Cock Buning, J. Buné en E. Eljon, *Jaarverslag 2018* (Hilversum, Commissariaat voor de Media, 2019) 17.

Consumenten moeten nieuws zelf op waarde kunnen schatten, maar van socialmediabedrijven wordt ook actie tegen desinformatie verwacht

FOTO US DEPARTMENT OF DEFENSE, KATIE LANGE

spreiden.[39] Dat zorgt voor een sterke toename van oncontroleerbare informatie.

Het uitgangspunt van de overheid is dat burgers zelf informatie op waarde kunnen schatten. De minister van BZK laat weten dat transparantie over de herkomst van informatie erg belangrijk is.[40] Daarom is het belangrijk dat de overheid sociale media betrekt bij de bestrijding van desinformatie. Tegenwoordig voeren ambtenaren regelmatig overleg met verschillende socialmediabedrijven over de bestrijding van desinformatie, onder meer met Google, Twitter, Microsoft, LinkedIn, Facebook, Mozilla et cetera. In een aantal gevallen maken ze afspraken, zoals het opstellen van een *code of conduct*. Hierbij valt te denken aan het verkrijgen van inzicht in de herkomst van politieke advertenties. Sommige van de geïnterviewde experts geloven niet direct in deze benadering, omdat naar hun mening het ethisch besef nog ontbreekt.

Socialmediaplatforms moeten zich realiseren dat het verspreiden van informatie niet ongelimiteerd kan plaatsvinden. Er bestaat ook nog een verantwoordelijkheid naar de gebruiker, de Nederlandse samenleving. Kortom, de toenemende populariteit van het internet werkt de verspreiding van desinformatie in de hand. Daar staat tegenover dat Nederland een zeer divers medialandschap kent, wat de kans op acceptatie van eenzijdige desinformatie verkleint. De Nederlandse overheid heeft ingezet op meer transparantie in online-nieuwsgaring.

Versterken informatiepositie

De minister van BZK heeft aangegeven dat samenwerking belangrijk is om verspreiding van desinformatie te kunnen monitoren. Op internationaal niveau is Nederland aangesloten bij verschillende fora, zoals het G7 Rapid Response Mechanism, het Integrity Security Initiative en de Counter Hybrid Support Teams. Hier worden op verschillende niveaus informatie en analyses uitgewisseld. Nederland is ook betrokken bij het European Centre of Excellence on Countering Hybrid Threats, waar ook de verspreiding van desinformatie aan de orde komt.[41] Bovendien participeert Nederland in het Strategic Communication Centre of Excellence in Riga (Litouwen)[42] en NATO's Cooperative

39 Rosen, 'A Most Useful Definition of Citizen Journalism'.

40 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief*, met kenmerk 2019-0000546545.

41 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief*, met kenmerk 2019-0000546545.

42 'About Us', website Strategic Communications Centre of Excellence (2019) zie: https://www.stratcomcoe.org/about-us-0.

Cyber Defence Centre of Excellence in Tallinn (Estland).[43] Op nationaal niveau komt eenmaal in de twee weken de interdepartementale werkgroep Desinformatie bijeen, voorgezeten door het ministerie van BZK. Deze werkgroep bestaat uit verschillende stakeholders, waaronder de Counter Hybrid Unit van Defensie, de NCTV, vertegenwoordigers van de ministeries van Buitenlandse Zaken, Justitie en Veiligheid, Onderwijs Cultuur en Wetenschap, Volksgezondheid, Welzijn en Sport en de veiligheidsdiensten. Deze werkgroep doorloopt regelmatig mogelijke dreigingsscenario's. Internationale en nationale samenwerkingsverbanden versterken het totaaloverzicht van eventuele verspreiding van desinformatie en werken aan een onderlinge band om samen ten strijde te trekken tegen desinformatie.

Reactie op desinformatie

De minister van BZK geeft duidelijk aan dat het reageren op desinformatie in de eerste plaats geen taak is van de overheid. De overheid treedt pas op als het om illegaal verkregen, onwettige of ontwrichtende informatie gaat, er een bedreiging is voor de politieke of economische stabiliteit van de Nederlandse samenleving of als de nationale veiligheid in het geding is. Het kabinetsbeleid is er wel op gericht betrokken partijen te stimuleren de herkomst en inhoud van informatie te onderzoeken. Bovendien vindt de minister het belangrijk een verhaal met een duidelijke boodschap (narratief) te hebben.[44] Een sterk verhaal maakt de boodschap immers aantrekkelijker en vergroot de kans op acceptatie.

De Nederlandse krijgsmacht

Deze paragraaf gaat in op de maatregelen die de Nederlandse krijgsmacht, als onderdeel van de Nederlandse overheid, heeft genomen. Het ministerie van Defensie is van oudsher een departement dat zich op de veiligheid van de Nederlandse samenleving richt en externe dreigingen monitort en bestudeert. De krijgsmacht, en vooral het Commando Landstrijdkrachten, studeert sinds de Russische annexatie van de Krim in 2014 op verschillende vormen van desinformatie. Het zijn deze onderzoekers die in een integrale aanpak van desinformatie een rol van betekenis kunnen spelen. Eén van de geïnterviewde experts met een militaire achtergrond gaf aan dat het besef van constante blootstelling aan desinformatie in Nederland nog onvoldoende is onderkend en dat er kansen liggen voor Defensie om dit te verbeteren. Defensie kan een signaalfunctie hebben binnen de Nederlandse overheid, die nodig is bij het tegengaan van desinformatie.

De Nederlandse krijgsmacht hamert ook op het belang van strategische communicatie. Volgens de *Nederlandse Defensie Doctrine* integreert strategische communicatie alle communicatiecapaciteiten in samenhang met andere militaire activiteiten. Hierdoor is het mogelijk de operationele omgeving te begrijpen en vorm te geven en om de doelgroep te informeren, overtuigen en beïnvloeden ter ondersteuning van de militaire doelstellingen.[45]
Maar in de praktijk schort het hier nogal eens aan. Vaak vertellen de militairen wel wie ze zijn en wat ze doen, maar verzuimt Defensie om verdere duiding te geven of om deel te nemen aan maatschappelijke discussies over veiligheidsvraagstukken. Militairen aarzelen vaak hun vakinhoudelijke kennis en inzichten te delen met de rest van Nederland; het wordt hun al snel te politiek. Daarmee laat de Nederlandse krijgsmacht kansen liggen om met een helder en geloofwaardig verhaal desinformatie tegen te gaan.[46]

Het antwoord op de vraag hoe militairen moeten reageren op desinformatie omvat volgens de geïnterviewde experts verscheidene belangrijke facetten. Ten eerste dient de individuele militair erop voorbereid te zijn dat hij of zij te maken krijgt met allerlei vormen van desinformatie. Opleidingen en onderwijs kunnen bij desinfor-

43 'About Us', website NATO Cooperative Cyber Defence Centre of Excellence (2020) zie: https://ccdcoe.org/about-us/.
44 Minister van Binnenlandse Zaken en Koninkrijksrelaties, *Kamerbrief,* met kenmerk 2019-0000546545.
45 Commandant der Strijdkrachten, *Nederlandse Defensie Doctrine* (Den Haag, ministerie van Defensie, 2019) 89.
46 Versteegden, *Resilience Can Counter Dezinformatsiya,* 41.

In de strijd tegen desinformatie moet Defensie de strategische communicatie goed op orde hebben, zodat de Nederlandse samenleving een duidelijk en begrijpelijk verhaal te horen krijgt

FOTO MCD, PAUL TOLENAAR

matiebewustzijn helpen. De Nederlandse Defensie Academie biedt al colleges *virtual warfare* en de minor *Info@War* aan. Daarnaast dienen militairen basislessen te krijgen over de werking van desinformatie. De experts zijn ook van mening dat militairen blootgesteld moeten worden aan desinformatie en andere vormen van misleiding om vervolgens uitgelegd te krijgen hoe dergelijke mechanismen werken. Dit vergroot de weerbaarheid.

Ten tweede is er het vraagstuk van bereidheid en capaciteit. Is de Nederlandse regering bereid militaire capaciteit in te zetten tegen desinformatie? Wellicht komt de regering met een dergelijk verzoek. Daarom moet de Defensiestaf nu al nadenken over de vraag of de krijgsmacht in staat is activiteiten uit te voeren gericht op het tegengaan van desinformatie. Of kan de krijgsmacht andere overheidsdiensten ondersteunen bij het uitvoeren van deze taak?

Ten slotte dient er volgens de geïnterviewde experts met een militaire achtergrond in de krijgsmacht een betere integratie plaats te vinden tussen het fysieke domein – het optreden met tanks, infanteristen, kanonnen, vliegtuigen en schepen – en de informatieomgeving om op een samenhangende manier op desinformatie te reageren. Elke activiteit is immers ook een vorm van communicatie, en Triple P is hierbij een belangrijk onderdeel: Presence, Posture and Profile. Hoe presenteert een eenheid zich tijdens een operatie? Wat straalt ze uit? Welke indruk laat zij na? Is een robuuste, afschrikwekkende of wellicht juist een sociaalvaardige indruk gewenst? Deze indruk dient in ieder geval goed te zijn afgestemd met de soort operatie en de wijze van beïnvloeding die de eenheid uitvoert.[47] Het gaat er om de opponent te beïnvloeden, en dat kan met *bombs and bullets*, maar ook met *bits, bytes and soundbites*. Ook op deze wijze zijn pogingen tot desinformatie van een opponent te bestrijden.

47 'All About Perception…', editoriaal in: *Militaire Spectator* 188 (2019) (7/8) 346.

Conclusie

In dit artikel stond de vraag centraal hoe de Nederlandse overheid en krijgsmacht omgaan met desinformatie. Desinformatie is gemanipuleerde informatie, die een verzender verspreidt met de bedoeling anderen te misleiden. Vaak is het lastig te achterhalen wat nu precies desinformatie is. Als twee mensen een gebeurtenis waarnemen en daarover berichten, is de kans immers groot dat er twee verschillende beschrijvingen van de gebeurtenis ontstaan. Is dan de ene beschrijving de waarheid? En is de andere beschrijving dan desinformatie? In Nederland heerst de overtuiging dat feit en fictie werkelijk te scheiden zijn, maar soms wordt vergeten dat andere gemeenschappen daar anders over denken, terwijl ook in Nederland de twijfel over dergelijke tweedelingen toeneemt.

Nederland wordt van buitenaf veelvuldig belaagd met allerlei vormen van gemanipuleerde informatie. Binnen de Nederlandse overheid is afgesproken dat de minister van BZK de kartrekker is bij het formuleren van beleid voor het tegengaan van desinformatie. De minister gaat begrijpelijkerwijs zorgvuldig met deze verantwoordelijkheid om, en wil niet in een politiek-gevoelig debat terechtkomen over wat wel of geen desinformatie is. Alleen als de politieke of economische stabiliteit van Nederland of de nationale veiligheid op het spel staan, moet de overheid ingrijpen.

Andere ministeries en overheidsorganisatie staan het ministerie van BZK bij in de bestrijding van desinformatie. Een valkuil bij deze interdepartementale samenwerking is dat de verschillende ministeries te veel hun eigen belang najagen. Het beleid tegen desinformatie begint desondanks vorm te krijgen, waarbij het bewustzijn van de burgers en bevordering van mediawijsheid centraal staan. In dat kader werkt de overheid hard aan vier verschillende programma's: bewustwording om weerbaarder te zijn tegen desinformatie, transparantie in het doen en laten van sociale media door afspraken met providers te maken, de informatiepositie versterken door nationaal en internationaal de handen ineen te slaan, en na te denken over hoe te reageren op vormen van desinformatie.

Er liggen kansen voor de Nederlandse krijgsmacht. Binnen het ministerie van Defensie is al veel onderzoek verricht naar beïnvloeding met informatie. Defensie zou in de Nederlandse interdepartementale aanpak van desinformatie naast een ondersteunende ook een adviserende en signalerende rol kunnen vervullen. Daarnaast moet het ministerie van Defensie de strategische communicatie goed op orde krijgen. Een duidelijk en begrijpelijk verhaal bij elke militaire operatie die de Nederlandse krijgsmacht verricht is een sterk wapen in de bestrijding van desinformatie. Bovendien dienen Nederlandse militairen bij oefeningen en operaties het fysieke domein en de informatieomgeving beter te integreren, waarbij Presence, Posture and Profile een belangrijk uitgangspunt is.

Waarschuwing

Wie de conclusie leest, ziet bij de overkoepelende aanpak van desinformatie ook een rol voor de krijgsmacht weggelegd. In de krijgsmacht gaan echter steeds meer stemmen op om zelf proactief desinformatiecampagnes te gaan uitvoeren wanneer – of wellicht voordat – de internationale spanningen oplopen. Maar dat is vragen om moeilijkheden. Want wie is de doelgroep? En welke 'desinformatie' wordt dan gedeeld? Dit soort gemanipuleerde informatie verspreidt zich wereldwijd en komt razendsnel ook bij de Nederlandse bevolking terecht. Informatie heeft nu eenmaal een andere ricochet-werking dan conventionele munitie. *Collateral damage* is niet te voorkomen en nadat de gemanipuleerde informatie de doelgroep heeft bereikt, verspreidt ze zich daarna snel. Deze informatie krijgt dan een boemerangeffect, waarbij de gemanipuleerde informatie terugkeert naar de eigen positie, ongemerkt de samenleving binnensluipt en daar veel angst en schade veroorzaakt. Hierdoor kunnen grote problemen ontstaan, want de Nederlandse bevolking wil nu eenmaal – direct of indirect – niet door haar overheid worden voorgelogen. De Nederlandse overheid, inclusief de krijgsmacht, dient te voorkomen dat ingezetenen door haar (des)informatiecampagne wanhopig uitroepen: 'Zeg me dat het niet zo is, … zeg me dat het niet waar is!' ■

Verdediging tegen imagefare

Het gebruik van beeldvorming als wapen

Imagefare wordt gebruikt om desinformatie te verspreiden. Het houdt in dat beeldvorming wordt ingezet als wapen ter vervanging van traditionele militaire middelen. Vooral in asymmetrische conflicten die veel media-aandacht genieten, komt imagefare voor. In westerse staten kan, door het democratische systeem, imagefare grote gevolgen hebben. Het is daarom van belang dat een westerse staat zich tegen imagefare kan wapenen. Dit artikel beschrijft en analyseert vier mogelijkheden om dit te doen: de negatieve beeldvorming beperken, de verspreiding van die beeldvorming stoppen, het betwisten van de betrouwbaarheid van de beeldvorming, en het ontwikkelen van een eigen narratief. Westerse staten kunnen vooral winst halen door negatieve beeldvorming te beperken, wat bereikt kan worden door op elk niveau en bij elke militaire activiteit rekening te houden met de perceptie die wordt gecreëerd. Daarnaast kan een staat door een eigen narratief te ontwikkelen de bevolking weerbaarder maken tegen beeldvorming van de opponent.

*Cadet-vaandrig mr. drs. S.A. van Hout**

Dat de heersende perceptie van een conflict bij het thuisfront van grote invloed kan zijn op het verloop van een conflict is niet nieuw. Beeldvorming, bijvoorbeeld door het gebruik van visuele beelden in de media, is hierbij van groot belang.[1] Zo is voor velen de foto van het meisje Kim Phúc, dat naakt en schreeuwend van de pijn wegrent na een napalmaanval door het Zuid-Vietnamese leger, misschien wel hét beeld van de Vietnamoorlog.[2]

Hoewel de term 'CNN-effect' zijn intrede pas deed tijdens de eerste Golfoorlog, werd met de komst van het nieuwe genre van fotojournalistiek, oorlogsfotografie, al geëxperimenteerd in de Frans-Duitse Oorlog. In het interbellum werd fotografie verder ontwikkeld en sinds de Spaanse Burgeroorlog, waarvan de dagelijkse verslaggeving in kranten gepaard ging met actuele foto's, speelt visueel beeldmateriaal een grote rol in de beeldvorming van een conflict. Met de komst van de televisie kwamen door technologische ontwikkelingen de beelden van conflicten nog meer de huiskamer binnen en bleken deze beelden een directe invloed op de publieke opinie te kunnen uitoefenen. De gekantelde publieke opinie in de Vietnamoorlog wordt vaak gekoppeld aan de visuele beelden van de oorlog die in het nieuws verschenen.[3]

Ook het beeldmateriaal van de dode Amerikaanse soldaat die door de straten van Mogadishu werd gesleept, ging de hele wereld over en kenmerkte het begin van het einde van de aanwezigheid van de Amerikaanse troepen in Somalië.[4] Beeldvorming kan dus een grote

* Sterre van Hout is alumnus van de master Military Strategic Studies aan de NLDA en volgt momenteel de Postacademische opleiding Militair Juridische Dienst Krijgsmacht. Dit artikel is geschreven naar aanleiding van een paper voor het vak Militaire Operaties I (Warfighting) dat zij in het kader van die opleiding heeft gevolgd. Zij bedankt kolonel drs. A.J.H. Bouwmeester voor zijn commentaar op eerdere versies.

1 Michael Griffin, 'Media Images of War', in: *Media, War & Conflict* 3 (2010) (1) 1.

2 Griffin, 'Media images of war', 13.

3 De invloed van beeldmateriaal op de publieke opinie en daarmee op het verloop van de Vietnamoorlog is in de academische literatuur betwist. Zie bijvoorbeeld Daniel C. Hallin, *The Uncensored War: The Media and Vietnam* (Berkeley, University of California Press, 1989); Piers Robinson, 'Theorizing the influence of media on world politics models of media influence on foreign policy', in: *European Journal of Communication* 16 (2001) (4) 523-544.

4 Steven Livingston, *Clarifying the CNN effect: An examination of media effects according to type of military intervention* (Cambridge, Harvard University, 1997) 15.

Imagefare wordt gebruikt om desinformatie te verspreiden en beeldvorming te beïnvloeden FOTO FLICKR

invloed hebben op het narratief en daarmee op het verloop van een conflict.

Door technologische ontwikkelingen zoals het internet en mobiele telefoons met camera is de stroom van informatie in de wereld gegroeid.[5] Door deze ontwikkelingen en nieuwe vormen van media zijn niet alleen conventionele media in staat om het narratief te bepalen, maar iedereen met een internetverbinding. Hiermee kan een staat of *non-state actor* (nsa) het narratief beïnvloeden of zelfs bepalen. Volgens Ayalon zijn in asymmetrische conflicten de media een belangrijk wapen geworden van moderne oorlogvoering.[6] De actor die het narratief van een conflict kan bepalen, heeft derhalve de heilige graal in handen.
Sommige landen en nsa's hebben dit beter begrepen dan westerse staten.[7] Zo is voor Al Qaida het informatiedomein het meest prominent, terwijl informatie voor westerse staten slechts een ondersteunende rol speelt in een conflict.[8] Daar komt nog eens bij dat westerse journalisten vaak gebonden zijn aan ethische journalistieke normen, waarbij waarheidsgetrouwe berichtgeving belangrijk is. Andere staten en nsa's voelen zich in hun beeldvorming of berichtgeving niet aan deze normen gebonden en gebruiken imagefare om een bepaald narratief te creëren. Omdat de stroom van informatie sneller en groter is geworden, is het van belang dat staten zich kunnen wapenen tegen deze narratieven die hun aan de 'slechte kant' van een conflict plaatsen.

Dit artikel onderzoekt en analyseert verschillende manieren waarop westerse staten zich kunnen verdedigen tegen imagefare, het inzetten van beeldvorming als wapen in een conflict, als alternatief voor traditionele militaire middelen. Hiertoe wordt eerst gekeken naar wat imagefare inhoudt en waarom het

5 Ami Ayalon, Elad Popavich en Moran Yarchi, 'From Warfare to Imagefare: How states should manage asymmetric conflicts with extensive media coverage', in: *Terrorism and Political Violence* 28 (2016) (2) 258.
6 Ayalon et al., 'From warfare to imagefare', 263.
7 Ibidem, 264.
8 David Kilcullen, *The accidental guerrilla: fighting small wars in the midst of a big one* (Oxford, Oxford University Press, 2009) 300.

vooral voor westerse staten van belang is om zich hiertegen te wapenen. Vervolgens worden verschillende mogelijkheden geanalyseerd hoe een westerse staat zich kan verdedigen tegen imagefare. Afsluitend komt aan de orde waar het zwaartepunt van westerse staten moet liggen in de verdediging tegen imagefare.

Imagefare

Het hybride conflict en imagefare

De term hybrid warfare kreeg bekendheid nadat de Israëlische strijdkrachten in 2006 niet bleken opgewassen tegen Hezbollah tijdens de Israëlisch-Libanese oorlog.[9] Volgens Hoffman gebruikte Hezbollah, een nsa, een combinatie van conventionele en onconventionele middelen en liet de beweging hiermee zien dat nsa's in staat kunnen zijn om kwetsbaarheden van westerse krijgsmachten te ontdekken en te gebruiken.[10] Een debat over de opkomst en betekenis van hybride conflictvoering volgde en groeide na de annexatie van de Krim door Rusland. De literatuur kent verschillende definities en aanduidingen van hybride oorlogvoering.[11] Wat de meeste definities met elkaar gemeen hebben is dat er bij een hybride conflict of dreiging zowel militaire als niet-militaire middelen worden ingezet om een strategisch doel te bereiken, waarbij desinformatie en misleiding een grote rol spelen.[12] Hybride conflictvoering veronderstelt een gewapend conflict waarin tegenstanders deze verschillende middelen tegelijkertijd inzetten, terwijl onder hybride dreiging juist het gebruik van niet-militaire middelen in vredessituaties wordt verstaan om zo het functioneren van een maatschappij te ondermijnen.[13] In dit artikel staat het hybride conflict centraal, aangezien imagefare tijdens een conflict wordt toegepast. Hybride conflicten worden dus niet slechts op het conventionele slagveld gewonnen of verloren, maar op verschillende fronten, waardoor de staat genoodzaakt is om meerdere machtsinstrumenten in te zetten. Bij deze geïntegreerde inzet kan gebruik worden gemaakt van diplomatieke machtsmiddelen, informatie als machtsmiddel, militaire machtsmiddelen en economische machtsmiddelen (DIME). In de gereedschapskist van de niet-militaire middelen die gebruikt kunnen worden in een conflict, zit dus ook het gebruik van het informatiedomein.[14] Imagefare maakt hier deel van uit.

FOTO ISRAEL DEFENSE FORCES

Een Israëlische militair maakt een Hezbollah-bunker onschadelijk in 2006. Dat conflict liet zien dat nsa's in staat zijn kwetsbaarheden van westerse krijgsmachten te gebruiken

Wat is imagefare?

In asymmetrische conflicten, waar een van de conflictpartijen inferieur is aan de ander voor wat betreft de fysieke militaire capaciteiten, kan de militair zwakkere partij toevlucht nemen tot het gebruik van beeldvorming om het conflict te winnen. Beeldvorming wordt derhalve ingezet als wapen om het gebrek aan voldoende militaire capaciteit te ondervangen. Imagefare wordt als volgt gedefinieerd: 'The use of images as a guiding principle or a substitute for traditional military means to achieve political objectives, or

9 Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007).
10 Hoffman, *Conflict in the 21st Century*, 35.
11 Zie: Hoffman, *Conflict in the 21st Century*; Kilcullen, *The accidental guerrilla*, 3; Russell W. Glenn 'Thoughts on "hybrid" conflict', in: *Small Wars Journal* (March 2009) 2. Zie: https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict.
12 NCTV, *Chimaera. Een duiding van het fenomeen 'hybride dreiging'* (Den Haag, NCTV, 2018) 3.
13 NCTV, *Chimaera,* 3.
14 NCTV, *Chimaera,* 3.

influence public perception about their conflict, and to achieve success on the image battlefield that plays an important role in modern conflict along with military confrontation.'[15]
Images zijn representaties van de werkelijkheid, die door woorden, beeldmateriaal, en daden kunnen worden overgebracht.[16] Onder images worden in imagefare dus niet enkel visuele beelden verstaan, maar ook de perceptie van een conflict die wordt overgebracht. In dit artikel wordt daarom voor images de term beeldvorming gebruikt. Visuele beelden hebben desalniettemin een grote invloed op de beeldvorming van een conflict.[17] 'Pictures speak louder than words', aldus Bolt.[18] Een enkele afbeelding lijkt het conflict te kunnen vatten en fungeert als een *short-cut* naar de essentie van een conflict.[19] Een visueel beeld kan namelijk complexe situaties versimpeld weergeven. Met het maken of vrijgeven van een visueel beeld wordt meer gedaan dan slechts de verslaggeving van een gebeurtenis. Visuele beelden van conflicten zijn gekleurd in de zin dat ze een 'goed' of 'fout' laten zien. Ze vertellen aan de ontvanger wie in het conflict de held is, en wie de schurk. De interpretatie van de afbeelding vormt een realiteit voor het publiek en speelt daarmee een grote rol in imagefare.[20]

Imagefare komt vooral voor in asymmetrische conflicten met veel media-aandacht.[21] Asymmetrische conflictvoering kan in dat geval ook een hybride conflict zijn, aangezien naast militaire middelen ook niet-militaire middelen worden ingezet om het gebrek aan militaire middelen op te heffen en omdat desinformatie een grote rol speelt. Kwetsbaarheden in de traditionele westerse manier van oorlogvoering worden hiermee blootgelegd. De media worden gebruikt om een bepaalde perceptie over te brengen. Zoals beschreven in de inleiding, is het gebruik van media in conflicten niet nieuw. Conflicten zijn gezien hun dramatische aard nieuwswaardige gebeurtenissen. In het algemeen richt het nieuws zich vaak op conflicten en wanorde.[22] Omdat opponenten in een conflict weten dat het conflict veel media-aandacht zal krijgen, wedijveren zij over hoe het conflict wordt geframed.[23] Zowel statelijke actoren als nsa's gebruiken de media om hun eigen handelen te legitimeren.[24] Bij het winnen van de hearts and minds, of dat nou bij het thuisfront is, de internationale gemeenschap of juist de opponent, speelt beeldvorming dus een grote rol.

Zowel statelijke actoren als nsa's gebruiken de media om hun eigen handelen te legitimeren

Bolt beschrijft in zijn boek *The violent image* dat insurgents door middel van beeldvorming alternatieve wereldbeelden onder het publiek kunnen verspreiden en plaatsen tegenover het narratief dat wordt uitgedragen door de staat.[25] Hierbij wordt ingespeeld op de emotie en aansluiting gezocht bij de cultuur en historie die in het collectief geheugen van het publiek zijn verankerd, met als gevolg dat deze alternatieve

15 Ayalon et al., 'From warfare to imagefare', 256.
16 James Farwell, *Persuasion and power, the art of strategic communication* (Washington, D.C., Georgetown University Press, 2012) 58-104.
17 M. Yarchi 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', in: *Media, War & Conflict* 9 (2016) (3) 292; Neville Bolt, *The violent image insurgent propaganda and the new revolutionaries* (New York, Columbia University Press, 2012) 130.
18 Bolt, *The violent image insurgent propaganda and the new revolutionaries,* 130.
19 Yarchi, 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', 292.
20 MCDC, *Military implementation of strategic communication in coalition operations - A practitioners handbook,* (2018) 3.
21 Ayalon et al., 'From warfare to imagefare', 256.
22 Yarchi, 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', 292.
23 Sarah Maltby, *Military media management: negotiating the 'front' line in Mediatized War* (Florence, Taylor & Francis Group, 2012) 109.
24 Yarchi 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', 295.
25 Bolt, *The violent image: insurgent propaganda and the new revolutionaries*, 130.

narratieven hout lijken te snijden bij het publiek. Hiermee wil de opponent de verhoudingen tussen het publiek en de regering op scherp stellen. Het gebruik van imagefare kan een voor de westerse staat ongunstig narratief over het conflict laten ontstaan of versterken en kan de westerse staat hiermee op flinke achterstand zetten in *the war on ideas*.[26]

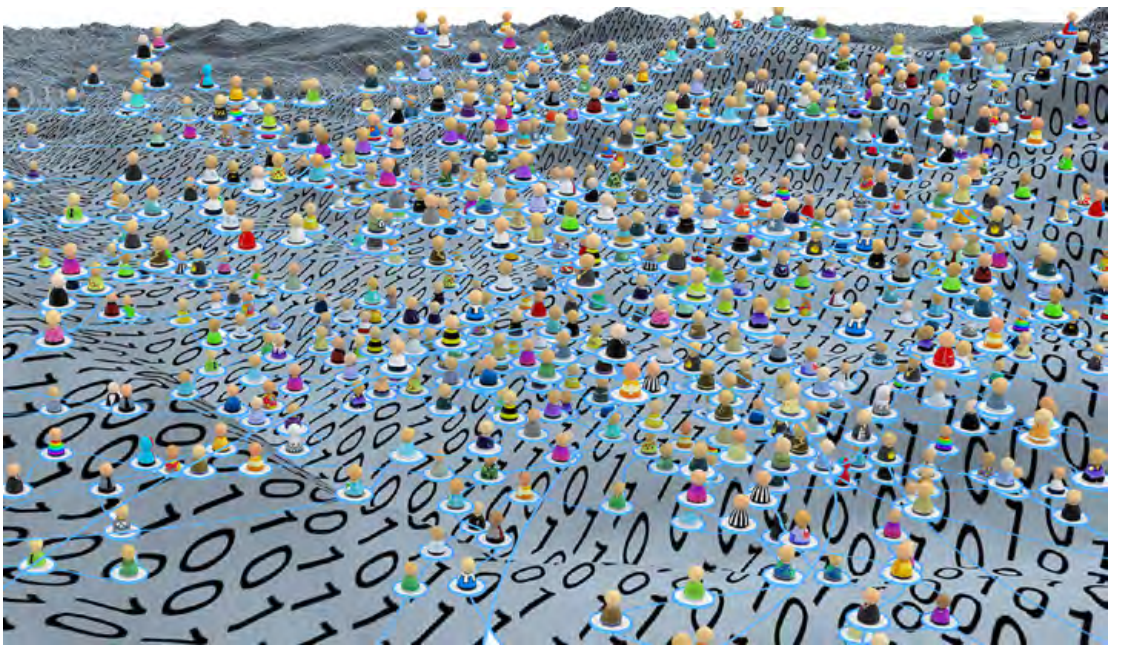
Imagefare moet worden onderscheiden van het CNN-effect, de veronderstelling dat de mainstream media besluitvorming over buitenlandbeleid in grote mate kunnen beïnvloeden.[27] Bij het CNN-effect gaat het om de reguliere media die verslag doen van een conflict of buitenlandse aangelegenheid. Bij imagefare gaat het om het gebruik van beeldvorming als vervanging van traditionele militaire middelen in een conflict door een partij in dat conflict. Reguliere mediavormen kunnen het effect van imagefare wel versterken als zij de beelden van de opponenten meenemen in hun nieuwsberichten. In dat geval komen de beelden immers bij een groter publiek terecht. Overigens wordt het CNN-effect in de literatuur genuanceerd.[28]

Wat imagefare relevant en actueel maakt is dat door technologische ontwikkelingen de informatiestroom enorm is toegenomen. Ook zijn er nieuwe vormen van media ontstaan, waarop iedereen met toegang tot internet beelden kan delen. Westerse journalisten zijn veelal gebonden aan ethische codes, maar in hedendaagse conflicten kan elk individu zijn eigen nieuws verspreiden en dus een bepaalde perceptie uitdragen. Als cyber-identiteiten, digitale weergaven van een individu of een groep, de perceptie van een conflict pogen te veranderen of beïnvloeden, spreken we van soft-cyberoperaties.[29] Dit is het geval als het internet wordt gebruikt om via socialemediaaccounts de perceptie te beïnvloeden.

De invloed van imagefare in democratieën

Juist in democratieën kan een bepaalde perceptie van een conflict dat door imagefare bij het publiek terecht komt een grote impact hebben. Dit heeft ten eerste te maken met het feit dat in democratieën vaak geen censuur bestaat, in tegenstelling tot autocratische staten. Elke inwoner kan daardoor worden blootgesteld aan beelden die een bepaalde kleur geven aan de werkelijkheid. Ten tweede kan het narratief dat wordt uitgedragen door beelden een indirect strategisch gevolg teweegbrengen in democratieën.[30] De kern van de democratie is namelijk volksvertegenwoordiging en de publieke opinie speelt in democratieën dan ook een grote rol.[31] Wanneer de bevolking merkt dat van de snelle overwinning die door de regering beloofd was geen sprake is, of als er bodybags terugkomen, groeit de weerstand tegen de inzet van militaire middelen in het conflict.[32] Bovendien blijkt dat in democratieën het maatschappelijk draagvlak voor het conflict daalt naarmate het conflict langer duurt.[33] Merkt een volksvertegenwoordiger dat het draagvlak binnen zijn of haar achterban afneemt, dan moet hij of zij hierover verantwoording afleggen en veranderingen doorvoeren om de achterban tevreden te houden.[34] De regering is hierdoor genoodzaakt zich te wenden tot middelen die de steun van de inwoners weer vergroten, wat soms betekent dat het beleid moet worden herzien. Dit niet alleen met het oog op het conflict zelf, maar ook omdat dit draagvlak van de achterban tevens een politiek of zelfs persoonlijk belang heeft. Verkiezingen in democratieën vinden immers regelmatig plaats. Autocratische staten hebben hier logischerwijs minder last van, aangezien de stem van het volk in mindere mate meetelt in beleidsvorming. Imagefare is daarom uitermate geschikt om te gebruiken tegen westerse staten. Het kan de publieke steun voor een conflict doen afbrokkelen en hiermee indirect het verloop van het conflict sturen.[35]

26 Yarchi, 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', 292.
27 Livingston, *Clarifying the CNN effect*, 1.
28 Zie bijvoorbeeld: Livingston, *Clarifying the CNN effect*; Piers Robinson, 'Theorizing the influence of media', 523-544.
29 Paul Ducheine en Jelle van Haaster, 'Een operationeel raamwerk voor cyberoperaties', in: *Militaire Spectator* 182 (2013) (12) 382.
30 Ayalon et al., 'From warfare to imagefare', 260.
31 Dan Reiter en Allan Stam, *Democracies at War* (Princeton, Princeton University Press, 2002) 148.
32 Reiter en Stam, *Democracies at War*, 148.
33 Ibidem, 159.
34 Ibidem, 148.
35 Ayalon et al., 'From warfare to imagefare', 260.



De informatiestroom is enorm toegenomen, waardoor imagefare een vlucht heeft genomen FOTO DARPA

Verdediging tegen imagefare

Voorheen richtten westerse staten zich vooral op kinetische operaties, waarbij de opponent met name in het fysieke domein werd aangepakt.[36] Langzamerhand wordt erkend dat *new school operations*, waar wapens niet alleen in het fysieke domein worden gezocht, maar ook in het informatiedomein, van groot belang zijn.[37] De focus van westerse staten op de fysieke component van militair vermogen heeft hun op achterstand gezet.[38] Het is duidelijk dat westerse staten het belang van imagefare moeten inzien en naar adequate mogelijkheden moeten zoeken om zich hiertegen te wapenen. Maar hoe kan een staat zich het beste wapenen tegen een beeldenoverstroming van een onbekende afzender die zich op het (sociale)mediafront bevindt? Imagefare kan niet worden uitgeroeid. Wel kan de beeldvorming gestuurd worden en kunnen de effecten van imagefare worden beperkt. In de literatuur zijn vier mogelijkheden te onderscheiden om dit te bereiken.

Negatieve beeldvorming beperken

Ten eerste heeft de staat de mogelijkheid om beeldvorming te beïnvloeden. Ayalon stelt dat, gezien het feit dat de informatiestroom niet meer te sturen is, beleidsmakers tijdens het plannen van militaire acties zich moeten laten leiden door mogelijk gebruik van imagefare door de opponent en de hieraan verbonden gevolgen.[39] Militaire optredens kunnen dan zodanig gepland en georkestreerd worden dat de kans op verspreiding van ongunstige beelden, die het narratief en daarmee de legitimiteit van het militair optreden in twijfel trekken, kleiner wordt. Het bewustzijn van de gevolgen van imagefare tijdens een conflict kan de acties van krijgsmachten direct beïnvloeden doordat zij ten gevolge van die aanwezigheid gaan handelen op een manier die de media en het thuisfront zal bevallen.[40] De taak ligt hier dus bij de krijgsmacht.

36 Peter Pijpers, 'De twitterende tegenstander. Een discours over de rol van mediaculturen in een conflict', in: *Militaire Spectator* 183 (2014) (6) 312.
37 Paul Ducheine, Jelle van Haaster en Richard van Harskamp, 'Manoeuvring and generating effects in the information environment', in: P.A. Ducheine en F. Osinga (red.), *Winning without killing, the strategic and operational utility of non-kinetic capabilities in crises* (Den Haag, Springer, 2017) 2.
38 Pijpers, 'De twitterende tegenstander', 312.
39 Ayalon et al., 'From warfare to imagefare', 256.
40 Maltby, *Military Media Management*, 102.

FOTO THE WHITE HOUSE

Bewerkte beelden, deep fakes, van wereldleiders kunnen grote internationale gevolgen hebben

Het Allied Command Transformation van de NAVO heeft in het kader van de Multinational Capability Development Campaign (MCDC) 2017-2018 een handboek samengesteld waarin uitgebreid wordt ingegaan op de wijzen waarop militair strategische communicatie kan worden toegepast in operaties.[41] Strategische communicatie heeft als doel het publiek van waarheidsgetrouwe informatie te voorzien met als gevolg dat het publiek wordt beïnvloed om de doelen van de informatiegever te ondersteunen.[42] In het handboek wordt omschreven dat bij elk aspect van militaire activiteiten communicatie een rol speelt, of dat nu gewenst is of niet.[43] Tijdens een conflict is de krijgsmacht, onbewust of bewust, continu in een strijd verwikkeld in het informatiedomein. De krijgsmacht speelt hier een rol als hoeder van het politieke narratief en moet ervoor zorgen dat het politieke doel gereflecteerd wordt in alle aspecten waarvan communicatie kan uitgaan bij militaire inzet. Het handboek suggereert dan ook dat informatie als een operationele factor moet worden beschouwd waarmee tijdens het gehele planningsproces rekening moet worden gehouden.[44] De communicatie die van militaire activiteiten uitgaat komt niet alleen terecht bij de opponent, maar ook media, het thuisfront, belanghebbenden en civiele partners kunnen ontvanger zijn. De situational awareness voor wat betreft het informatiedomein dient dus te worden vergroot. Dit kan door een geïntegreerde communicatiebenadering, waarbij communicatie op elk niveau meegenomen wordt in de planning en de uitvoering van militaire activiteiten. Van commandanten van hoog tot laag wordt verwacht dat zij een proactieve houding hebben ten aanzien van strategische communicatie en dat ze ervoor zorgen dat het oogmerk van de hogere commandant, waar het gaat om communicatie, weerklinkt in de planning en uitvoering.

Het verkleinen van de kans op negatieve beeldvorming is niet in alle gevallen mogelijk. Zoals hierboven is uitgelegd kan ook een neutrale situatie geframed worden zodat die een bepaald gevoel opwekt bij de ontvanger van het beeld, terwijl deze beeldvorming niet in overeenstemming is met de werkelijkheid. Voorts bieden de groeiende technologie en de toegang tot het internet mogelijkheden om gefotoshopte beelden te verspreiden. Ook is het voorkomen van negatieve beeldvorming door strategische communicatie geen oplossing voor deep fakes: video's of audiobestanden die door kunstmatige intelligentie zodanig bewerkt zijn dat het lijkt alsof een persoon bepaalde dingen zegt of doet die hij in werkelijkheid niet heeft gezegd of gedaan. Deze beelden en audiofragmenten zijn dermate realistisch, dat de betrouwbaarheid ervan niet direct te betwisten is. De verwachting is dat deep fakes in de toekomst worden ingezet als militair middel door grootmachten als Rusland, China, de Verenigde Staten en nsa's.[45] Het inzetten van deep fakes kan grote consequenties hebben. Hierbij valt bijvoorbeeld te denken aan bewerkte beelden waarop militairen oorlogsmisdaden lijken te plegen, wat een kanteling van de publieke opinie over het conflict tot gevolg kan hebben. Maar ook het

41 MCDC, *Military implementation of strategic communication in coalition operations*.
42 James Stavridis, 'Strategic communication and national security', in: *Joint Forces Quarterly* (2007) (46) 7.
43 MCDC, *Military implementation of strategic communication in coalition operations*, 3.
44 Ibidem, 6.
45 Stew Magnuson, '"Deep Fakes" Will Only Thicken the Fog of War', in: *National Defense* 59 (2020) (3) 5.

geval dat een wereldleider lijkt aan te kondigen dat militair ingrijpen voorhanden is, kan grote interstatelijke spanningen tot gevolg hebben en zelfs de wereldorde bedreigen.[46]

Verspreiding van beeldvorming stoppen

Een tweede mogelijkheid om imagefare te beperken is het stoppen van de verspreiding van beeldvorming. Met name visuele beelden worden wanneer zij gebruikt worden voor imagefare via verschillende kanalen veelvuldig gedeeld. Socialemediakanalen als Twitter en Facebook zijn actief bezig om accounts te sluiten die nepnieuws verspreiden.[47] Echter, de verspreiders anticiperen hierop. Zo bleek dat Islamitische Staat (IS), die Twitter gebruikt om te rekruteren en zijn ideologie te propaganderen, elke keer na het sluiten van een account een nieuw account aanmaakte dat snel in het netwerk van de volgers van het oude account werd geïntegreerd.[48] Op deze manier kon IS tot halverwege 2014 ervoor zorgen dat het sluiten van de Twitteraccounts de informatiestroom niet of nauwelijks beperkte. Bovendien pasten de gebruikers de inhoud van berichten zo aan dat ze voldeden aan de richtlijnen van Twitter en daardoor minder snel gedetecteerd werden.

Een ander voorbeeld is Rusland, dat in Sint-Petersburg een 'trollenfabriek' heeft staan. Het personeel verspreidt en deelt zoveel mogelijk fake news via verschillende kanalen.[49] Daarnaast worden bots ingezet, computerprogramma's die berichten bijvoorbeeld snel kunnen retweeten, waardoor de berichten een groter publiek bereiken.[50]

Het verminderen van de stroom aan berichten is dus een omvangrijke taak. Bovendien zijn staten hierbij afhankelijk van socialemediabedrijven als Facebook en Twitter, de platformen waar de beelden worden gedeeld. Daarnaast sluiten deze platformen een account slechts in het geval dat gebruikersrichtlijnen worden geschonden. Beelden of berichten die zodanig geframed worden dat ze een voor de staat ongunstige perceptie uitdragen, maar wel enigszins op de werkelijkheid berusten, vallen hier niet onder. Een andere manier om verspreiding van negatieve beeldvorming te stoppen, is het actief optreden door de staat in de vorm van elektronische oorlogvoering en het uitvoeren van cyberoperaties.[51]

Het betwisten van de betrouwbaarheid van de beeldvorming

Ten derde kan het waarheidsgehalte van de beeldvorming worden betwist, om zo de effecten van imagefare te beperken.[52] Dit is echter makkelijker gezegd dan gedaan. Hoewel het belangrijk is voor westerse staten om ongunstige beeldvorming van een conflict van context te voorzien, is het kwaad veelal geschied op het moment dat beelden en berichtgeving in de media zijn verspreid. Het publiek heeft zijn opinie over het conflict dan al gevormd. Dit komt mede door het bestaan van *anchoring*, de *bias* die ervoor zorgt dat individuen meer waarde hechten aan informatie die als eerste beschikbaar is gesteld.[53] Aanvullende informatie wordt dan in het licht van de eerder beschikbaar gestelde informatie geïnterpreteerd. De eerste indruk is lastig te weerleggen en pogingen hiertoe zijn zelden effectief.[54] Dit geldt des te meer omdat de term fake news te pas en te onpas wordt gebruikt, waardoor mensen minder snel geneigd zijn, als bepaalde beeldvorming uiteindelijk dit stempel krijgt, dit te geloven. Dat berichtgeving of beelden die verspreid zijn als zodanig worden geclassificeerd, betekent dus niet dat de publieke opinie daarmee direct gekanteld wordt.[55] Ook kan er enige tijd overheen gaan voordat de betrouwbaarheid van de berichtgeving of beelden, bijvoorbeeld bij deep fakes, is onderzocht. Gedurende deze tijd kan de

46 Nina Schick, '"Deep Fake" Videos Threaten the World Order: We must Prepare for an Age when AI Allows Anyone with a Grudge to Create Convincing Bogus Clips', in: *The Times* (27 februari 2019).

47 NATO StratCom COE, *Social media as a tool of Warfare* (Riga, NATO StratCom COE, 2016) 35.

48 NATO StratCom COE, *Social media as a tool of Warfare,* 38.

49 Ibidem, 28.

50 Ibidem, 25.

51 C. Paul en M. Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model* (Santa Monica, RAND Cooperation, 2016) 11.

52 NATO StratCom COE, *Social media as a tool of Warfare,* 20.

53 Blair Williams, 'Heuristics and biases in military decision making', in: *Military Review* 90 (2010) (5), 48.

54 Paul en Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model*, 9.

55 Yarchi 'Does using "imagefare" as a state's strategy in asymmetric conflicts improve its foreign media coverage?', 295.

Nederlandse militairen patrouilleren in Mali. Voor een succesvol narratief moet het doel van militaire inzet duidelijk zijn

FOTO MCD, GERBEN VAN ES

beeldvorming al snel verspreid worden en kan de staat niet in een eerste reactie de gebeurtenissen zoals weergegeven ontkennen en hiermee geruchten de kop indrukken. Dit kan vervolgens bij de bevolking overkomen als een bevestiging van hetgene dat wordt afgebeeld, want wie zwijgt, stemt toe.

Overigens is het bestrijden van het waarheidsgehalte slechts mogelijk in het geval dat de beelden of berichtgeving ook daadwerkelijk een ander beeld vertonen dan de werkelijkheid. Van de foto's die naar buiten kwamen van de Abu Ghraibgevangenis, die blijk gaven van de misstanden die daar hadden plaatsgevonden, kon het waarheidsgehalte simpelweg niet worden betwist. De effecten van de beeldvorming kunnen in dat geval moeizaam worden beperkt.

Een eigen narratief

Een vierde mogelijkheid is het creëren van een eigen narratief. Om op deze wijze een eigen perceptie van het conflict aan de wereld te laten zien, is niet alleen cruciaal om te bereiken dat militaire operaties als een nationaal succes worden gezien.[56] Zoals hierboven genoemd kan strategische communicatie namelijk ook het thuisfront als ontvanger hebben. Het hebben van een sterk en geloofwaardig narratief tegenover het thuisfront kan tot gevolg hebben dat er mentale weerbaarheid ontstaat bij de eigen bevolking tegen het narratief van een opponent, dat door imagefare bij de ontvangers terechtkomt.[57]

Weerbaarheid is het vermogen van een sociaal systeem om zich voor te bereiden op verstoringen, het herstellen na verstoringen en om zich aan te passen en te groeien nadat een verstoring is opgetreden.[58] Aangezien in hybride conflicten desinformatie en misleiding een grote rol spelen, moet mentale weerbaarheid meer

56 Ayalon et al., 'From warfare to imagefare', 261.

57 NCTV, *Chimaera,* 31; Theo Brinkel, 'The Resilient Mind-Set and Deterrence', in: P. Ducheine en F. Osinga (red.), *Netherlands Annual Review of Military Studies, Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises* (Den Haag, T.M.C. Asser Press, 2017) 35.

58 Judith Rodin, *The Resilience Dividend; Managing Disruption, Avoiding Disaster, and Growing Stronger in an Unpredictable World* (Londen, Profilebooks, 2014) 3.

Hoe bestendiger het narratief van de staat is, des te lastiger dit is te betwisten met imagefare

aandacht krijgen, oftewel, hoe een maatschappij weerbaar kan zijn tegen desinformatie en misleiding door middel van berichtgeving en beeldvorming.[59] Mentale weerbaarheid kan onder andere vergroot worden door het versterken van het narratief van de staat over hoe het conflict gepercipieerd moet worden.[60] Hoe bestendiger het narratief van de staat is, des te lastiger het is voor de opponent om dit narratief door middel van imagefare te betwisten.[61] Is het narratief dat een staat uitdraagt juist wankel, tegenstrijdig of niet zichtbaar, dan zal imagefare eerder effect sorteren bij het thuisfront, met alle gevolgen van dien.[62] Hierbij is, zoals hiervoor besproken, van belang dat in het planningsproces op elk niveau rekening wordt gehouden met het beeld dat de krijgsmacht tijdens een conflict wil uitdragen, met welk verhaal er moet worden verteld. Dit eigen narratief van de westerse staat kan verspreid worden door middel van de eerder besproken strategische communicatie.[63] Het thuisfront is dan de ontvanger van de communicatie. Ook kunnen staten een gezamenlijk narratief uitdragen, wat geopperd wordt in het NCTV-rapport *Chimaera.*[64] Een narratief moet aan bepaalde eisen voldoen, wil het invloed hebben op de weerbaarheid van de bevolking.

Ten eerste moet het narratief op strategisch niveau overeenkomen met het narratief dat op operationeel en zelfs op tactisch niveau wordt neergezet. [65] Bestaat hier discrepantie, dan gaat dat ten koste van de geloofwaardigheid. De Graaf noemt in dit verband ook dat een strategisch narratief consistent en coherent moet zijn.[66] Als belangrijke elementen van een gekozen narratief vaak aangepast worden neemt de geloofwaardigheid van het narratief af. Als er dan een counternarratief bestaat, dat een meer consistent en coherent verhaal vertelt over het verloop van het conflict en duidelijker laat zien wie de held en wie de schurk is in het conflict, is de bevolking eerder geneigd uit te gaan van deze beeldvorming. Ten tweede moet er voor de inzet van militaire middelen een duidelijk doel worden gecommuniceerd.[67] Het is cruciaal dat een ondubbelzinnige reden kan worden gegeven voor de inzet. Wanneer die er niet is, blijft de bevolking met vragen zitten die de opponent maar al te graag wil beantwoorden. Ook het vooruitzicht op succes moet worden gecommuniceerd.[68] Wordt dit nagelaten dan zal de steun voor de militaire inzet sneller afnemen. Ten slotte moet het narratief ook feitelijk en verifieerbaar zijn.[69] Natuurlijk kan de realiteit het narratief inhalen en moet het misschien worden bijgesteld, maar de bevolking moet erop kunnen vertrouwen dat wat de staat verkondigt op waarheid berust.[70] Het probleem bij het uitdragen van een eigen narratief is dat de zender geen controle meer heeft over de interpretatie van elementen van het narratief.[71] Hierdoor kunnen verschillende ontvangers een narratief op verschillende manieren inter-

59 Theo Brinkel, 'Moraliteit, beleid en weerbaarheid', in: *Militaire Spectator* 187 (2018) (7/8) 384; Brinkel, 'The Resilient Mind-Set and Deterrence', 27.

60 Cees van Doorn, *Societal resilience and an answer to disinformation: The case of flight MH17* (Breda, Nederlandse Defensie Academie, 2019) 16.

61 Bolt, *The violent image*, 79.

62 Ibidem, 79.

63 Stavridis, 'Strategic communication and national security', 7.

64 NCTV, *Chimaera,* 31.

65 Stavridis, 'Strategic communication and national security', 5-7; Beatrice de Graaf, George Dimitriu en Jens Ringsmose (red.), *Strategic narratives, public opinion, and war: winning domestic support for the Afghan war* (Londen, Routledge, 2015) 8.

66 De Graaf et al., *Strategic narratives, public opinion, and war,* 8.

67 Ibidem, 9.

68 Ibidem, 9.

69 Lawrence Freedman, 'The possibilities and limits of strategic narratives', in: Beatrice de Graaf, George Dimitriu en Jens Ringsmose (red.), *Strategic narratives, public opinion, and war: winning domestic support for the Afghan war* (Londen, Routledge, 2015) 24.

70 Freedman, 'The possibilities and limits of strategic narratives', 24.

71 Ibidem, 26.

preteren. Om dit tegen te gaan is het belangrijk dat het narratief aansluit bij de cultuur en geschiedenis van het publiek.

Het risico van het uitdragen van een sterk narratief om imagefare tegen te gaan, is dat het bestempeld kan worden als propaganda, een omstreden begrip dat wordt geassocieerd met misleiding en het verspreiden van leugens.[72] Wanneer een narratief dit stempel krijgt, staat de geloofwaardigheid ervan direct op het spel. Om deze reden is het van groot belang dat de staat een balans vindt tussen transparantie en de noodzaak om te communiceren met de bijbedoeling de bevolking een bepaald beeld op te leggen.[73]

Conclusie

Dit artikel heeft gepoogd verscheidene manieren uiteen te zetten waarop westerse staten zich kunnen wapenen tegen imagefare. Hiertoe is eerst uiteengezet wat imagefare inhoudt en welke relatie het heeft met hybride conflictvoering. Besproken is dat met name beeldmateriaal een perceptie kan beïnvloeden. Daarna is ingegaan op de gevolgen die imagefare teweeg kunnen brengen en waarom het juist voor westerse staten, gezien de invloed die de publieke opinie heeft op de besluitvorming, belangrijk is zich hiertegen te verdedigen. Vier mogelijkheden zijn geanalyseerd die een westerse staat heeft om beeldvorming van de opponent te sturen en de gevolgen van imagefare te beperken.

Hoewel de ene mogelijkheid meer effect kan sorteren dan de andere, is het van belang dat de verschillende manieren in samenspel kunnen worden gebruikt. Het stoppen van informatiestromen en het tegenspreken van een narratief zijn beide omvangrijke en lastige taken, omdat het stoppen van informatiestromen nagenoeg onmogelijk is en tegenspreken van een narratief vaak niet een gewenst effect heeft. De voornaamste oplossing lijkt gevonden te kunnen worden in het gebruik maken van het feit dat media overal aanwezig zijn, door middel van de zichtbare militaire operaties op een dergelijke manier uit te voeren dat een negatieve beeldvorming minder snel kan ontstaan. Bewustzijn moet worden gecreëerd dat van elke militaire activiteit communicatie uitgaat. Dit begint al bij het plannen van een operatie. Hoewel ongewenste beeldvorming door framing, fotoshop en deep fakes niet kan worden uitgesloten, wordt de kans kleiner dat er ongunstig waarheidsgetrouw beeldmateriaal naar buiten wordt gebracht, waarvan beleidsmakers de inhoud niet kunnen betwisten. Daarnaast is het van belang dat westerse staten zelf een sterk narratief bepalen en dit uitdragen richting het thuisfront. Door het uitdragen van een eigen narratief wordt de eigen bevolking weerbaarder tegen beeldvorming die een ander verhaal lijkt te verkondigen. Een grotere aanwezigheid van de krijgsmacht op sociale media is bijvoorbeeld productiever dan pogingen om de informatie van de opponent te verzwakken of de verspreiding ervan te limiteren.[74]

Westerse staten moeten dus meer van zich laten horen. De stilte aan het 'westerse front' kan westerse staten op achterstand zetten in de hybride conflicten van vandaag de dag. Van elk militair aspect en activiteit gaat communicatie uit en als een staat niets doet om de communicatie te sturen met als doel een bepaald beeld uit te dragen, dan vervult de tegenstander die rol wel. Een westerse staat kan het zich simpelweg niet meer permitteren om stil te blijven. Westerse staten moeten dus bij het plannen van militaire operaties communicatie een leidende rol laten spelen, zodat negatieve beeldvorming zoveel mogelijk wordt beperkt. Daarnaast is het van groot belang dat er actiever gebruik wordt gemaakt van het informatiedomein om een sterk eigen narratief uit te dragen richting de bevolking, waardoor het volk als het ware wordt gewapend tegen het gebruik van imagefare door de opponent. Op deze wijze kunnen westerse staten zich verdedigen tegen imagefare, waarvan het gebruik de komende jaren ongetwijfeld alleen maar zal toenemen. ■

72 Farwell, *Persuasion and power,* 23.
73 Farwell, *Persuasion and power,* 35.
74 NATO StratCom COE, *Social media as a tool of Warfare,* 25.

Dezinformatsiya in Lithuania

A seemingly charming fairy tale with elves and trolls

Following Russia's annexation of Crimea in 2014 and the conflict in the southeast region of Ukraine, NATO deployed four battlegroups to Poland and the Baltic States. The Netherlands contributes troops to the battlegroup in Lithuania, which considers itself a 'front state' against the Russian Federation. Lithuania is a desirable target for Russian disinformation campaigns. How is the country targeted by Russia, and how does Lithuania protect itself? This article provides an explanation for Russian disinformation, or *dezinformatsiya*, its history, and how it is related to other known terms, such as active measures. It is paramount for societies, including the Dutch, to be well aware of the likelyhood of being targeted by Russian dezinformatsiya campaigns.

Colonel Han Bouwmeester[*]

'You cannot fight lies with lies', says Ričardas Savukynas, a Lithuanian elf, 'when I see there are propaganda movements which are directed at the preparation of war, I need to do something!'[1] Savukynas' concern shows the kind of conflict nations are involved in today. It also depicts the tense atmosphere between the Baltic states and the Russian Federation over the past six years. The Baltics are seriously targeted by Russian influence campaigns, since Mother Russia still feels responsible for the safety of the ethnic-Russians and Russian speakers in the Baltics.[2] In Estonia and Latvia more

* Colonel Han Bouwmeester is an Associate Professor of Military Strategy and Land Operations at the Netherlands Defence Academy. Colonel Bouwmeester is currently finalising his PhD-research on modern Russian deception warfare and this article is a sneak preview of his dissertation.

1 NATO, 'Elves vs Trolls – Fighting Disinformation in Lithuania', YouTube, 3 May 2017. See: https://www.youtube.com/watch?v=KDsrwSX7piw.

2 Agnia Grigas, *Beyond Crimea: The New Russian Empire* (New Haven, CT (USA), Yale University Press, 2016) 136; Ofer Fridman, *Russian Hybrid Warfare: Resurgence and Politicisation* (London (UK), Hurst & Company, 2018) 171.

than a quarter of the population is ethnic-Russian, although in Lithuania it is only about five per cent.[3] Lithuania is, in a different way, a desirable target for Russian disinformation; it borders on the Russian exclave of Kaliningrad and contains, together with Poland, the so-called Suwalki corridor: flat terrain between Belarus and Kaliningrad that may function as a perfect link-up passage for Russian troops if necessary.[4]

Following Russia's annexation of Crimea in 2014 and the conflict in the Donbas, the southeast region of Ukraine, member-states at NATO's

3 Jörg Noll et al, 'De Baltische Staten, de Russische Minderheden en de Verdediging van de NAVO', in: *Militaire Spectator* 186 (2017) (4) 173.

4 Viljar Veelen, 'Why It Would Be Strategically Rational for Russia to Escalate in Kaliningrad and the Suwalki Corridor', in: *Comparative Strategy* 38 (2019) (3) 182-197.

Dutch F-16s in Lithuania participate in NATO's Baltic Air Policing mission

PHOTO MCD, HILLE HILLINGA

2016 Warsaw summit agreed to forward deploy four multinational battlegroups to the Baltics and Poland.[5] In 2017, the Netherlands armed forces largely contributed to the security of the Baltic states. It deployed four Dutch F-16s participating in the Baltic Air Policing task, one raiding squadron of marines for the Very High Readiness Joint Task Force, two ships and a submarine to the Standing Naval Forces and one infantry company as part of the German-led battlegroup in Lithuania.[6] Today, 270 Dutch military personnel are still attached to the battlegroup and stationed in Rukla, Lithuania, as 'reassurance measures' for eastern European Allies in NATO.[7] The Netherlands makes a significant contribution to the protection of NATO territory in the Baltics, and should therefore be aware of potential threats. In 2018, Christian Kamphuis warned in his *Militaire Spectator* article that Dutch troops in Lithuania are a likely potential target for Russian smear campaigns. Kamphuis described an incident in which Dutch soldiers, based in Lithuania, were falsely accused of being publicly drunk and disorderly.[8] In other words, Russia's disinformation campaigns targeted against the Baltics are also of interest to the Netherlands. If only because the Netherlands can easily get involved, this article will concentrate on the following question: How are Russian disinformation campaigns used against Lithuania?

To answer this question, this article will provide an explanation for Russian disinformation, or *dezinformatsiya*, its history and how it is related to other known terms, such as active measures, propaganda and *kompromat*. It also shows present-day appearances of dezinformatsiya and details how Russian authorities are currently harassing Lithuania, and how Lithuania is protecting itself.

A description of dezinformatsiya

To determine what kind of disinformation the Russian Federation uses against Lithuania, the concept of dezinformatsiya must be scrutinised first. Van den Herik, Molendijk and Bouwmeester already made a distinction in their article between mis-, dis- and malinformation.[9] Disinformation is a carefully crafted message to mislead the decision-making elite or the public, with every message at least partially conforming to generally accepted beliefs. Without a considerable degree of plausible information, it is difficult to gain the victim's confidence.[10] Otherwise the disinformation will not be accepted by its target audience.[11] Today the concept of dezinformatsiya is still used by Russian authorities and is reframed by Western experts as 'Kremlin's Weaponization of Information'.[12] Russian authorities use two different types of disinformation. The first category is offensive disinformation used to influence foreign decision-makers and public opinion abroad. The second category includes defensive disinformation, which Russian authorities employ to influence their own citizens.[13] This form of disinformation is primarily intended to combat the interference of the West in Russian society. Chief of Staff of the Russian armed forces Valery Gerasimov stated that the West, especially the United States, is using 'weapons of mass disorganization', such as cyber, media, intelligence services and diplomacy, to upset Russian society.

5 North Atlantic Treaty Organisation, Factsheet 'NATO's Enhanced Forward Presence', May 2017. See: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/1705-factsheet-efp.pdf.

6 Anne Bakker, 'Dutch Perspectives on the Security of the Baltic States', *Clingendael Spectator*, 20 December 2017. See: https://spectator.clingendael.org/nl/publicatie/dutch-perspectives-security-baltic-states.

7 Netherlands Ministry of Defence, 'Current Missions', 8 June 2020. See: https://english.defensie.nl/topics/missions-abroad/current-missions.

8 Christian Kamphuis, 'Reflexive Control: The Relevance of a 50-year-old Russian Theory Regarding Perception Control', in: *Militaire Spectator* 187 (2018) (6) 337.

9 Bo van den Herik, Tine Molendijk and Han Bouwmeester, 'Zeg me dat het niet waar is…? Een zoektocht naar Nederlands beleid en de rol van de krijgsmacht tegen desinformatie', in: *Militaire Spectator* 189 (2020) (9) 418-429.

10 Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (McLean, VA (USA), Pergamont-Brassey's International Defense Publishers, 1984) 49.

11 Ladislav Bittman, *The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare*, Syracuse University Research Corporation (New York, NY (USA), Ballantine Books/Random House, 1972) 20.

12 Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, A special report presented by The Interpreter, Institute of Modern Russia, November 2014.

13 Jon White, *Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation*, Policy Brief, Issue 2016/13, (Brussels (BEL), *Vrije Universiteit Brussel*, Jean Monnet Centre for Excellence, Institute for European Studies, 2016).

Gerasimov considered these new conflict methods as a modern Trojan Horse.[14]

History of dezinformatsiya

The origin of dezinformatsiya is still debatable. Some experts are convinced that Joseph Stalin decided that disinformation should look as if it were originally French. He organized an information campaign in which the word dezinformatsiya seemed to be derived from the French language, being a portmanteau of the words 'des' and 'information'. It was a meaningless expression, but another form of Russian ruse. Stalin made believe that dezinformatsiya was a French 'capitalist' tool targeted against the peaceful people of the Soviet Union.[15] Soviet intelligence officer Walter Krivitsky, who was born as Samuel Ginsberg and served in Germany, Poland, Austria, Italy, Hungary, and the Netherlands, had another view on the origin of dezinformatsiya, dating it back to the First World War. The German armed forces established a General Staff's Disinformation Service to disseminate improper information and news in order to confuse their adversaries. The first Soviet secret service adopted the term and the underlying techniques and used it for its own purposes. It translated the term into dezinformatsiya. [16]

14 Frans van Nijnatten, 'Het antwoord van Gerasimov op het Paard van Troje' in: *Militaire Spectator* 188 (2019) (7/8) 394.

15 Ion Mihai Pacepa, *Disinformation: Former Spy Reveals Secret Strategies for Undermining Freedom, Attacking Religion and Promoting Terrorism* (Washington, DC (USA), WND Books, 2013) 39.

16 Walter Krivitsky, *In Stalin's Secret Service*, Reprint (Frederick, MD (USA), University Publications of America, 1967) 234.

The Ukrainian military base in Crimea was surrounded by 'little green men', who were supported by a Russian dezinformatsiya campaign

PHOTO WIKIMEDIA COMMONS

While there had been successes during the early Cold War, dezinformatsiya did not catch on until the early 1960s. After the establishment of KGB's Department D in 1959,[17] the unit was directly connected to the Presidium of the Soviet Communist Party, and its main task was the dissemination of dezinformatsiya. Department D consisted of forty to fifty personnel, divided by region and function. In 1962, Department D was upgraded to the status of a service, Service A, under direct supervision of the First Chief Directorate of the KGB. Ivan Agayants, a legendary KGB officer, became Chief of Service A. Five years after its foundation, Service A managed nearly 400 dezinformatsiya operations per year. Agayants had a strict policy of recruiting new personnel involved in the conduct of dezinformatsiya operations. A new agent needed to be able to think creatively, culturally empathically, and out-of-the-box, alongside possessing personal characteristics such as rigour, self-discipline and ideological determination.[18]

During the 1980s the Soviets often dealt with the use of dezinformatsiya in an opportunistic manner. Unplanned incidents were seized upon by the Soviet KGB to launch a major dezinformatsiya campaign. Examples include incidents such as the attack on Pope John Paul II in 1981 by a Turkish terrorist, which was regarded as a CIA retaliation. Another example is the shooting of the Korean airliner with flight number KAL007 over the Kamchatka Peninsula in 1983 by a Soviet Sukhoi Su-15 interceptor jet, resulting in 269 fatalities. This incident was initially surrounded by conflicting reports and eventually dismissed as a purely defensive measure that had been hard to avoid.[19]

After the dissolution of the Soviet Union, the interest of the West in dezinformatsiya faded into the background, but that suddenly changed after the annexation of Crimea in 2014. At the time, the World was shocked to see how masked soldiers in uniforms without insignias, later referred to as 'little green men' by the Western media, could take over an entire peninsula belonging to Ukraine without firing a shot. The action was attributed to the Russian Federation, but the Russian authorities remained silent and initially denied their involvement. The activities of the little green men were supported by a dezinformatsiya campaign, which came not only from the Russian media but also from Russian politicians. For example, in April 2014, Russian Foreign Minister Sergei Lavrov accused the West of being the initiator of all the unrest in Ukraine in order to get more control in the region.[20]

Relation with active measures

The Soviet Union and the Russian Federation have a long tradition of misleading groups of people with manipulated information. With roots in Leninist thinking, mainly aimed at controlling their own population and influencing public opinion, the Soviets developed a series of deceptive activities that invariably included terms such as dezinformatsiya, active measures, propaganda, and kompromat.[21] The question now is whether these are all different concepts. The answer is simply 'no', although these terms partly overlap, which is explained in the following sections. It is striking that these concepts are again widely used in Russian dezinformatsiya operations today.

Some Russian and Western experts in information warfare use the term dezinformatsiya to refer to what the Soviet leaders called 'active measures'.[22] Although active measures are considered as just another term for dezinformatsiya, they are not quite the same. Dezinformatsiya is merely one of the overt and covert influencing practices used by the Soviet

17 KGB stands for *Komitet Gosudarstvennoy Bezopasnosti*, or Committee for State Security, the Soviet Secret Service.

18 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London (UK), Profile Books, Ltd, 2020) 145-146.

19 Michael Voslensky, 'The Empire of Lies', in: Raymond Sleeper, *Mesmerized by the Bear: The Soviet Strategy of Deception* (New York, NY (USA), Dodd, Meade & Company, 1987) 33.

20 Steve Rosenberg, 'Ukraine Crisis: West Wants to "Seize Control" – Russia', *BBC News*, 25 April 2014. See: https://www.bbc.com/news/world-europe-27153909.

21 Steve Abrams, 'Beyond Propaganda: Soviet Active Measures in Putin's Russia', in: *Connections: The Quarterly Journal* 15 (2016) (1) 7.

22 Richard Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (McLean, VA (USA), Pergamon-Brassey's International Defense Publishers, 1984) 39.

and later by the Russian leadership in these so-called active measures.[23] Soviet authorities viewed dezinformatsiya as a strategic weapon, useful in their overall active measure strategy. In turn active measures, or *aktivnyye meropriyatiya,* is a Soviet term for active intelligence operations to influence world events in order to reach one's own geopolitical aim.[24]

Retired KGB General Oleg Kalugin saw dezinformatsiya as one of the critical components of active measures, together with subversive activities. Kalugin viewed subversion as 'active measures to weaken the West, to drive wedges in Western community alliances of all sorts […] [and] sow discord among allies'.[25] Active measures focused on and exploited opponents' vulnerabilities in order to expand Soviet influence and power around the globe.[26] Active measures vary from media forgeries to messages that can cause reactions with various degrees of violence. Active measures are broader than only disinformation, they include propaganda, subversive activities, counterfeiting official documents, disinformation operations leading to assassinations, agents of influence, political domination, and various forms of religious suppression.[27] Today the 'old' active measures are still present in current Russian activities, they only look different. Current active measures include modern dezinformatsiya and subversion methods, such as deploying Orthodox priests, Russian government-funded news media outlets like RT and Sputnik, spies and 'computer hackers to ride and help create the wave of populist anger'.[28]

Relation with propaganda

Propaganda has a specific position within dezinformatsiya. In 1935, Leonard Doob, Professor of Psychology at Yale University, concluded that most propaganda uses stereotyping and suggestion. Stereotyping is the process in which people create mental images about human character traits and appearances and use these images to judge other people. In the case of propaganda, the propagandist constructs a picture or a narrative that his target group is ready to wholeheartedly accept.[29] This construction can be used as a stimulus to generate a suggestion, which affects people's reaction and behaviour, and often their attitude.[30] A Harvard University study into Nazi propaganda emphasized the contrast between 'Us versus Them' as the main theme in propaganda.[31] The propagandist ('Us') tries to persuade the public by intensifying his own 'good', using glorifying wording, and downplaying his own 'bad', while he also intensifies the other party's ('Them') 'bad', using denigrating language, and downplaying the other's party's 'good', denying its positive behaviour and actions.[32] The Russians know two specific forms of propaganda: *agitprop* and *spetspropaganda*.

> It is striking that Soviet concepts are again widely used in Russian dezinformatsiya operations today

23 Nicolas Cull et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It, An Analytic Report with Lessons for the Present* (London (UK), London School of Economics and Political Science, LSE-consulting, 2017) 18.

24 Aristedes Mahairas and Mikhail Dvilyanski, 'Disinformation - Дезинформация (Dezinformatsiya)', in: *The Cyber Defense Review* 3 (2018) (3) 21.

25 Oleg Kalugin, op. cit. in: Mahaireas and Mikhail Dvilyanski, *Disinformation*, 21.

26 Bittman, *The Deception Game*, 4-5; Matthew Lauder, *Truth is the First Casualty of War: A Brief Examination of Russian Informational Conflict during the 2014 Crisis in Ukraine*, Scientific Letter, DRDC-RDDC-2014-L262, (Ottawa (CAN), Defence Research and Development Canada, 2014) 3.

27 Vasili Mitrokhin and Christopher Andrew, *The Mitrokhin Archives: The KGB in Europe* (London (UK), Penguin Books, 2000) E-Book.

28 Or Honig and Ido Yahel, 'The Art of "Subversive Conquest": How States Take over Sovereign Territories Without Using Military Force', in: *Comparative Strategy* 36 (2017) (4) 294.

29 Leonard Doob, *Propaganda: Its Psychology and Technique* (New York, NY (USA), Henry Holt and Company, 1935) 35-37.

30 Leonard Doob, *Propaganda*, 51-56.

31 Karthik Narayanaswami, *Analysis of Nazi Propaganda: A Behavioral Study* (Cambridge, MA (USA), Harvard University, Faculty of Arts&Sciences, 2017) 4.

32 Hugh Rank, 'Teaching about Public Persuasion: Rationale and Schema', in: Daniel Dietrich (ed), *Teaching about Doublespeak* (Urbana, IL (USA), National Council of Teachers of English, 1976) 3-20.

Lithuanian President Gitanas Nauseda visited 'General Silvestras Zukauskas' Training Area in Pabrade and met with Lithuanian, German and United States troops and evaluated their readiness PHOTO OFFICE OF THE PRESIDENT OF THE REPUBLIC OF LITHUANIA

Agitprop is a portmanteau of 'agitation' and 'propaganda'. Agitation indicates the emotional part of propaganda, referring to how the message is received and to the mental state of the receiver. Propaganda, on the other hand, refers to the framing of the message and the way the message should be disseminated.[33] Agitprop is a form of political propaganda, especially communist, which was often used during the Soviet era. Emotional agitation puts the recipient in a condition in which he will act erratically and in a non-rational way. In order to reach a large audience, agitprop is spread to the general public through popular information channels, like literature, plays, movies, pamphlets, paintings and other art forms that all carry political messages, overtly or covertly.[34]

Spetspropaganda, which is short for 'special propaganda', was first taught in 1942 as a separate subject at the Military Institute of Foreign Languages in Moscow. It was removed from the curriculum in 1990 but reintroduced in 2000 after the institute had been reorganized.[35] Spetspropganda was used for blocking influence and for applying pressure and manipulation. The Soviets used spetspropaganda in line with the social-technical principles of successful propaganda, which were: (1) the principle of a massive and long-lasting impact, (2) the principle of believing desired and manipulated information, (3) the principle of supposed obviousness, and (4) the principal of emotional agitation, like agitprop.[36] The creation of dezinformatsiya, agitprop and spetspropaganda did not stop after the collapse of the Soviet Union. These forms of influencing are still used by Russian authorities today. Established Russian media platforms, such as RT,[37] together with

33 Han Bouwmeester, 'Lo and Behold Let the Truth Be Told: Russian Deception Warfare in Crimea and Ukraine and the Return of "Maskirovka" and "Reflexive Control Theory"', in: Paul Ducheine and Frans Osinga (eds), *Netherlands Annual Review of Military Studies 2017 (NLARMS 2017), Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises* (The Hague (NLD), Springer/T.M.C. Asser Press, 2017) 138.

34 Peter Kenez, *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917-1929* (Cambridge (UK), Cambridge University Press, 1985) 251-255.

35 Viktoria Margaryan, 'Russian Information Warfare', (2014). See: https://www.academia.edu/9596147/Russian_information_warfare.

36 Jolanta Darczweska, *The Anatomy of Russian Information Warfare: The Crimea,* Point of View Nr 24, (Warsaw (POL), Centre for Eastern Studies, 2014) 25.

37 'RT' is formerly known as 'Russia Today'.

news agencies, such as Sputnik and Rossiya Segodny, create and disseminate story lines, frames, agitprop and spetspropaganda. These media outlets are still at the heart of Russia's activities in the information environment.[38]

Relation with kompromat

Kompromat, meaning 'compromising material', is a special brand of dezinformatsiya, and refers to discrediting information that can 'be collected, stored, traded, or used strategically across all domains: political, electoral, legal, professional, judicial, media, or business.' Russian kompromat operations are machinations exercised through the circulation of often 'unsubstantiated or unproven information' (documents, messages, files, etcetera), which are destructive for all those involved. Kompromat has four ideal types, the first of which entails revelations about a victim's political activities, such as abuse of power, discrediting connections, and political disloyalty. The second type involves a victim's disreputable, sometimes illegal, economic activities, such as distrusted apportionment of budgets, fraudulent bank deals, capital flight, and preferential treatment in business agreements. The third type comprises accusations of victims taking part in criminal activities, including organized crime, contract killing, spying, tapping, and blackmail. The fourth type of kompromat contains revelations about a victim's private life, especially the ones that were created to discredit the victim. This type includes details of illegitimate income or property, sexual behaviour, sexual orientation, health, and misbehaviour of family members of the victim. Kompromat does not necessarily have to be manipulated information, as the four types of kompromat mentioned, but may also be factual and accurate. To give an example of kompromat: in the summer of 1997 the Russian Minister of Justice, Valentin Kovalev, was removed from his position after a Russian newspaper, *Sovershenno Sekretno*, showed certain pictures with Kovalev in the arms of prostitutes in a sauna controlled by a criminal group called Solntsevskaia. The minister insisted that he was lured into a trap. [39]

Current appearances

Contemporary Russian activities in the information environment, including dezinformatsiya campaigns, are designed along the four elements of former disinformation operations, also known as the 4-D approach: dismiss, distort, distract, and dismay.[40] In 2007 Alexandr Bedritsky, a Russian strategist, wrote that the key of current Russian warfare is not to destroy the enemy's morale or psyche or bring about physical destruction, but rather to form such a perception of reality that would be in line with Russian interests.[41] It may be argued that the contemporary way in which information and intelligence are gathered and possible opponents are manipulated makes Russia's disinformation operations very effective. Russia's covert activities include espionage, hacking, stealing, and laundering; it's semi-covert actions consist, among other activities, of troll deeds, forgery, disruption, and amplification, while the overt method is to provide propaganda pushers and fake news launderers with improper information.[42] Erik Donkersloot rightly argued in his *Militaire Spectato*r article that 'Russian operations are mostly designed to disrupt hostile societies and fuel internal polarization in target nations'.[43] In line with these intentions, the tactics of Russian authorities are rather to confuse than to convince a target audience, and to divide opinions instead of providing new insights. By creating many different storylines, Russian authorities attempt to deny the

38 Edward Lucas and Peter Pomerantsev, *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in in Central and Eastern Europe*, A Report by CEPA's Information Warfare Project in Partnership with the Legathum Institute, (August 2016), 6.

39 Alena Ledeneva, *How Russia Really Works: The Informal Practices that Shaped Post-Soviet Politics and Business* (Ithaca, NY (USA), Cornell University Press, 2006) 58-56.

40 Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, (Washington, DC (USA), Institute for the Study of War, 2015) 12-13.

41 Alexandr Bedritsky, *Realization of the Concepts of Information Warfare by Military and Political Leadership of the USA during the Modern Era* (Moscow (RF), Russian Institute for Strategic Studies (RISI), 2007).

42 Max Bergmann and Carolyn Kenney, *War by Other Means: Russian Active Measures and the Weaponization of Information* (Washington, DC, Center for American Progress, June 2017).

43 Erik Donkersloot, 'Hybrid Threats from the East: The Gerasimov Doctrine and Intelligence Challenges for NATO', in: *Militaire Spectator* 186 (2017) (9) 395.

audiences the ability to distinguish between truth and falsehood. On the other hand, the spokesperson of the Russian Ministry of Foreign Affairs often raised concerns about the risk of disinformation in the Western media, in which the Russian Federation is portrayed very negatively, and brazenly called on the United Nations to formulate a global strategy against disinformation and fabricated news.[44]

Kremlin Trolls

Dezinformatsiya operations can be conducted by Russian politicians and diplomats, mainstream media, non-governmental organisations (NGOs), or through cultural programmes and other means. One of the notable ways of distributing dezinformatsiya is through social media by the so-called bots, automated social media accounts, and 'Kremlin Trolls', fake social media accounts managed by Russian volunteers.[45] The Kremlin Trolls are part of the Russian Internet Research Agency (IRA). The IRA began its operations in 2013 in Saint Petersburg. From the start, the agency was run as a sophisticated marketing bureau in centralised office surroundings in Russia's second city. The IRA employed and trained over a thousand people to conduct round-the-clock influence operations.[46] The IRA has often been called the 'Troll Farm' or the

44 Alexander Averin, 'Russia and its Many Truths', in: Jente Althuis and Leonie Haiden (eds), *Fake News: A Roadmap* (Riga (LTV), NATO Strategic Communications Centre of Excellence/London (UK), The King's Centre for Strategic Communications, 2018) 59-60.

45 Todd Helmus, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Addendum (Santa Monica, CA (USA), RAND Corporation, 2018) 3.

46 Renée DiResta et al, *The Tactics & Tropes of the Internet Research Agency*, A Report Supported by the United States Senate Select Committee on Intelligence (Austin, TX (USA), New Knowledge, 2018) 6.

Lithuanian military personnel during NATO's exercise Winter Wolf PHOTO NATO

'Russian Troll Factory'.[47] The agency started out as the IRA and was later called Teka. Nowadays it is called Glavset, which was legally formed in 2015. It is interesting to note that Glavset's corporate address is in Rostov-on-Don, but its physical address is in Saint Petersburg. Glavset is housed and financially supported by Yevgeny Prigozhin, also appropriately known as 'Putin's Chef', as the President personally chose his company to cater several of his exclusive presidential receptions and dinners. Members of Glavset mask their internet activities using proxy servers and other anonymizers in order to astroturf.[48] Their main products are propaganda, fake news, and trolling, which is writing controversial reactions on comment sections of an article on the internet.[49]

The trolls or operators at Glavset work in twelve-hour shifts, on a 24/7 basis. The individual operators run multiple fake accounts and are expected to produce around fifty comments on news articles every day. Other operators maintain six Facebook accounts, posting three times daily about news and discussing new developments in Facebook groups twice a day, with a target of at least 500 subscribers at the end of the first month. On Twitter, operators run around ten accounts with up to 2,000 followers each and producing at least fifty tweets daily. The ones making comments are required to make 135 remarks during their shift. These operators are provided with five keywords or topics to use in their posting in order to stand out in search engines, as a result of which internet users end up on earlier postings.[50] The ultimate goal of the Kremlin Trolls is to initiate a gradual process of undermining Western democracies and disrupting democratic institutions in those nations.

It is strongly believed that the Kremlin Trolls first targeted Ukrainian and Russian citizens and, subsequently, American citizens well before the United States elections in 2016.[51] Today, there is a strong suspicion worldwide that the Kremlin Trolls have played a misleading role in the conflict in the Donbass, in the narratives surrounding the cause of the downing of flight MH17, and furthermore they are accused of having been involved in the Brexit referendum,[52] the 2016 American elections, and leaking correspondence of French President Emmanuel Macron's La République En Marche! ('The Republic That Works!').[53] Some nuance is needed in simply blaming the Kremlin Trolls for undermining Western democratic processes. In 2019, United States Special Counsel Robert Mueller declared that there was inadequate proof for a formal accusation of Russian authorities and their Kremlin Trolls.[54]

Dezinformatsiya campaigns in Lithuania

Like the two other Baltic states, Lithuania was one of the few former Soviet states to join the EU and NATO in 2004. After the annexation of Crimea in 2014, the Lithuanian government strongly disapproved of this Russian action. It became one of the chief advocates for an EU

47 Adrian Chen, 'The Agency', *New York Times Magazine*, 2 June 2015. See: https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

48 'Astroturfing' is the practice of masking the originator of a message to make it appear as though it derives from and is supported by a grassroots participant.

49 Joel Harding, 'Glavset is the New Name for Russian Internet Research Agency: The Russian Troll Farm', *To Inform is to Influence*, 10 September 2017. See: https://toinformistoinfluence.wordpress.com/2017/09/10/glavset-is-new-name-for-russian-internet-research-agency-the-russian-troll-farm/.

50 Andrew Dawson and Martin Innes, 'How Russia's Internet Research Agency Built Its Disinformation Campaign', in: *The Political Quarterly* 90 (2019) (2) 246; John Gallacher and Rolf Fredheim, 'Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas But Spread Pro-regime Messages at Home', in: Sebastian Bay (ed), *Responding to Cognitive Security Challenges* (Riga (LTV), NATO Strategic Communications Centre of Excellence, 2019) 61-80.

51 DiResta, *The Tactics & Tropes*, 6.

52 Georgina Lee, 'Here Is What We Know About Alleged Russian Involvement in Brexit', 4 News, *Channel 4*, 16 November 2017. See: https://www.channel4.com/news/factcheck/heres-what-we-know-about-alleged-russian-involvement-in-brexit; Nick Cohen, 'Why Isn't There Greater Outrage about Russia's Involvement in Brexit?', *The Guardian*, 17 June 2018. See: https://www.theguardian.com/commentisfree/2018/jun/17/why-isnt-there-greater-outrage-about-russian-involvement-in-brexit; Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump and Facebook Broke Democracy and How It Can Happen Again* (New York, NY (USA), HarperCollins Publishers, 2019) 333-353.

53 Andy Greenberg, 'Don't Pin the Macron Email Hack on Russia Just Yet', *Wired*, 5 August 2017. See: https://www.wired.com/2017/05/dont-pin-macron-email-hack-russia-just-yet/.

54 United States Department of Justice (US DOJ), 'Special Counsel Robert S. Mueller III Makes Statement on Investigation into Russian Interference in the 2016 Presidential Election', 29 May 2019. See: https://www.justice.gov/opa/speech/special-counsel-robert-s-mueller-iii-makes-statement-investigation-russian-interference.

treaty with Ukraine and it is highly supportive of the EU sanctions against the Russian Federation and eager to assist Ukraine. Lithuania is also part of the *avant-garde* of NATO member states in raising awareness about Russian threats. Over the last six years, Lithuania has increasingly developed a frosty relationship with the Russian Federation.[55] As a counter-reaction, Russian authorities targeted the Lithuanian society with several dezinformatsiya campaigns, sometimes in the form of spetspropganda. 'The Russian authorities try to create a manipulated history that denies Lithuania's right to exist', a top Lithuanian official explained in the British newspaper *The Guardian*.[56] Examples are the spreading of rumours that Lithuania's capital of Vilnius should not belong to Lithuania because it was Polish territory in the interwar period of the past century, and Klaipėdia, Lithuania's third largest bridge, never belonged to Lithuania but is supposed to be Russian property since it was a gift from Stalin.[57]

Over the last two years, Facebook has become one of the most important battlefields for dezinformatsiya operations. The Kremlin Trolls increased their efforts to polarise Lithuanian public opinion. The methods they use are known from previous online activities. Rather than pushing certain narratives, the Kremlin Trolls are disrupting public discourse by adopting extremist positions on both sides of Lithuania's political spectrum, thereby attempting to split Lithuanian society, often by exploiting already sensitive and existing divisive topics. Kremlin Trolls also tried to influence demonstrations in Lithuania by using social media, such as Facebook, prior to the demonstrations. Kremlin Trolls' working methods tend to start in neutral groups on Facebook, such as fan groups of pop stars or famous actors; accounts that attract a large number of followers. The posts in these Facebook groups are initially related to the subject of the group, and then slowly but steadily dezinformatsiya is actively inserted between neutral posts, thereby exposing the entire community belonging to that Facebook group to malicious disinformation. Kremlin Trolls usually organise their activities through VKontakte, the Russian version of Facebook, and then engage on Facebook.[58] Although Facebook is their favourite platform, Kremlin Trolls are also active on other social media platforms, such as YouTube, Instagram, Tumblr, Snapchat, Pinterest and Linkedin.[59]

During the spring of 2020 coronavirus-related information incidents grew over time and the Lithuanian population and NATO troops remained the main target of the dezinformatsiya campaign. Since the start of the COVID-19 pandemic, Kremlin Trolls have become increasingly active in using the opportunity to spread dezinformatsiya. Between February and April 2020, Lithuanian authorities identified a total of 869 coronavirus-related information incidents of various types, not only in Lithuanian, but also in Russian and English. Those who spread disinformation seek to capitalise on the COVID-19 pandemic to sow fear and tensions and turn public opinion against NATO troops in Lithuania.[60] The disinformation used is often a combination of agitprop and kompromat. In January 2020 a source, supposedly a Kremlin Troll, posted a made-up story on Lithuanian news website Kauno.diena.lt, or Kaunas Day, claiming that an American soldier of the U.S. Army's 1st Cavalry Division based in Lithuania, was diagnosed with COVID-19. The story was removed after having been online for just a couple of minutes. In March 2020, a manipulated narrative was posted on the Baltic web portal Delfi.lt, claiming that the massive Allied Defender Exercise 2020, recently scaled back due to

55 Kremlin Watch, 'Lithuania', June 2020. See: https://www.kremlinwatch.eu/countries-compared-states/lithuania/.

56 Emma Graham-Harrison and Daniel Boffey, 'Lithuania Fears Russian Propaganda is Prelude to Eventual Invasion', *The Guardian*, 3 April 2017. See: https://www.theguardian.com/world/2017/apr/03/lithuania-fears-russian-propaganda-is-prelude-to-eventual-invasion.

57 Graham-Harrison and Boffey, 'Lithuania Fears Russian Propaganda'.

58 Jacob Willemo, *Trends and Developments in the Malicious Use of Social Media* (Riga (LTV), NATO Strategic Communications Centre of Excellence, 2019) 25.

59 Keir Giles, James Sherr and Anthony Seaboyer, *Russian Reflexive Control* (Kingston, Ontario (CAN), Royal Military College of Canada, Defence Research and Development Canada, 2018) 30; Christian Bell, *Use of Social Media as an Effort*, Multinational Capability Development Campaign, (Mayen (GER), Zentrum für Operative Kommunikation der Bundeswehr, 2016).

60 BNS/TBT Staff, 'Lithuanian Military Warns of Increase in Coronavirus-related Disinformation', *The Baltic Times*, 27 April 2020. See: https://www.baltictimes.com/lithuanian_military_warns_of_increase_in_coronavirus-related_disinformation/.

COVID-19 precautions, would still take place in Lithuania, but secretly.[61] In April 2020, a falsified statement of NATO Secretary General Jens Stoltenberg on the alleged withdrawal of NATO troops from Lithuania due the corona-crisis was sent by email across Lithuania to the press, government, as well as the NATO Headquarters in Brussels and the Lithuanian Defence Ministry.[62] These notifications are just a few examples of a larger dezinformatsiya campaign launched in an opportunistic abuse of the corona-crisis.

Lithuanian response

Russia's aggression against Ukraine in 2014 caused a paradigm change in Lithuania's strategic culture. One of the most significant impacts has been that defence took centre stage in political and societal life in a way not witnessed before in Lithuania since its independence in 1990. The state of the Lithuanian armed forces (LAF) came under intense scrutiny. Since 2014, the Lithuanian defence budget has grown with 20-30 per cent annually, making it the fastest growth in the world. As part of the changes, Lithuania instated conscription, which immediately sparked a huge wave of potential participants.[63] The current LAF consists of Land, Air and Naval Forces, a Special Operations Force, Military Police, a Logistics Command and a Training and Doctrine Command. The LAF includes about 20,000 soldiers in active service, while almost 6,000 reserve soldiers are part of the National Defence Volunteer Forces (NDVF).[64] Lithuania considers itself a 'front state' against the Russian Federation, with the LAF and NDVF being the armed nucleus of all its defence activities. The Lithuanian defence system is based on the concept of 'total and unconditional defence', as required by Lithuania's 2012 National Security Strategy.[65]

Part of the change process was a latitude for security subcultures promoting non-military instruments, such as strategic communication and sophisticated cyber protection. A few years ago, members of the Lithuanian Special Operation Forces branch decided to establish the LAF Strategic Communications Department. In the meantime, this department has transformed into a unit with a civil-military structure. They have since become the top choice for Lithuanian public media regulators in seeking expert advice on suspected violations by Russian media of Lithuanian laws prohibiting war propaganda, or incitement to ethnic hatred. In addition, the employees of the department have become masters in detecting dezinformatsiya and all Russian media news transactions are closely monitored.[66] Today, the department also has far-reaching authority, such as the closing down of websites.[67]

Besides these initiatives by the government, other steps have been taken to counter dezinformatsiya in Lithuania. The first private fact-checking initiatives in the country have emerged. The news portal 15min.lt runs a fact-checking initiative called Patikrina 15 min, checking news items, as the name implies, every 15 minutes, a project launched in 2016 by journalist Liepa Zelniene. Another project was established in 2017 by Delfi.lt, the biggest news portal in Lithuania. Delfi.lt started collaboration with the military, journalists and civil society in detecting dezinformatsiya on the website Demaskuok.lt, which has also been funded by Google Digital Innovation Fund. In addition, totally different initiatives have also been launched. That is how media literacy became a

61 Patrick Tucker, 'Russia Pushing Coronavirus Lies as Part of Anti-NATO Influence Ops in Europe, *Defence One*, 26 March 2020. See: https://www.defenseone.com/technology/2020/03/russia-pushing-coronavirus-lies-part-anti-nato-influence-ops-europe/164140/.

62 Baltic News Service Staff, 'Fake News on NATO withdrawal from Lithuania Sent to Media, Brussels, *LRT*, 22 April 2020. See: https://www.lrt.lt/en/news-in-english/19/1166199/fake-news-on-nato-withdrawal-from-lithuania-sent-to-media-brussels.

63 Kristine Atmante, Riina Kaljurand and Tomas Jermalavičius, 'Strategic Cultures of the Baltic States: The Impact of Russia's New Wars', in: Katalin Miklóssy and Hanna Smith (eds), *Strategic Culture in Russia's Neighborhood: Change and Continuity in an In-Between Space* (Lanham, MD (USA), Lexington Books, 2019) 67-69.

64 International Institute for Strategic Studies (IISS), *The Military Balance 2019* (London (UK), IISS, 2019) 125.

65 Masha Hedberg and Andres Kasekamp, 'Baltic States', in: Hugo Meijer and Marco Wyss (eds), *The Handbook of European Defence Policies & Armed Forces* (Oxford (UK), Oxford University Press, 2018) 226.

66 Atmante, Kaljurand and Jermalavičius, 'Strategic Cultures of the Baltic States', 67-69.

67 VPRO Tegenlicht, 'Aan het Front van de Informatieoorlog', Directed by Mea Dols de Jong, 17 May 2020. See: https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2019-2020/aan-het-front-van-de-informatieoorlog.html.

Dutch military personnel of NATO's eFP exercise in Lithuania

PHOTO MCD, JASPER VEROLME

hot topic in Lithuania. Together with critical thinking they are two of the top priorities in the Lithuanian government's programme for the eradication of dezinformatsiya. The national strategy *Lithuania 2030* aims to introduce media literacy programmes in all education institutions, from nursery schools to universities.[68]

An important part of Lithuania's counter-disinformation strategy is that it does not only include government initiatives, but it extends well into the wider Lithuanian society. An example of these initiatives is the so-called 'elves', volunteers who set out to combat Kremlin Trolls, under the motto 'elves can beat the trolls'. The size of the elves' community changes constantly, but numbers in the thousands, and it includes journalists, IT professionals, businesspeople, students, and scientists. They all participate for a good cause: to prevent the Russian authorities and Kremlin Trolls from carrying out malicious dezinformatsiya campaigns in Lithuania. The elves consider themselves a movement, not an organisation. Their aim is to expose and combat false claims and contested narratives as quickly as possible. There are different types of elves, some of which are debunkers of manipulated information, while others run 'blame and shame' online campaigns against the Kremlin Trolls. In the *Financial Times* one of the elves stated: 'In Lithuania we work in one direction, even with the media, which normally are competitors. When we need to defend our country against propaganda and dezinformatsiya, we are united!'[69]

Conclusion

This article focused on the question: How are Russian disinformation campaigns used against Lithuania? Russian disinformation, or dezinfor-

68 Viktor Denisenko, 'Lithuania: Disinformation Resilience Index', Ukrainian Prism Foreign Policy Council, 31 July 2018. See: http://prismua.org/en/9065-2/.

69 Michael Peel, 'Fake News: How Lithuania's "Elves" Take on Russian Trolls', *Financial Times*, 4 February 2019. See: https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf.

matsiya, can be considered as a carefully crafted message to deceive the decision-making elite or the public of a target nation, community or group of people, with every message of disinformation at least partially conforming to generally accepted beliefs. Dezinformatsiya is not a modern invention but has been practised since the Soviet era and most dezinformatsiya operations are conducted by Russian politicians and diplomats, NGOs, the mainstream media and nowadays also frequently by Kremlin Trolls on social media. The main goal of these dezinformatsiya operations is to disrupt Western democracies, especially the three Baltic states. Since the Baltic states are both NATO and EU members, the dezinformatsiya problem is also becoming a concern for these two organisations and their member states.

Over the past six years, since the annexation of Crimea, Lithuania has seen an increase in the dezinformatsiya campaigns of the Russian authorities. They do not like Lithuania's membership of the EU and NATO and regard the immediate proximity of these two organisations as a threat to their own stability. To do something about this threat the Russian authorities frequently target Lithuania's population with dezinformatsiya, including non-factual information, spetspropaganda, agitprop and kompromat, in order to create disarray and chaos in Lithuanian society. However, it is not the only reason for Russian dezinformatsiya operations in Lithuania. Russian authorities are also seeking to drive a wedge between the population and foreign troops stationed in Lithuania under NATO's enhanced Forward Presence (eFP), including Dutch military personnel. On top of that, the Russians do not shrink from being opportunistic and spread all sorts of slander about COVID-19 in Lithuania.

In Lithuania, a special Strategic Communications Department has been established within the Lithuanian armed forces to detect and, if necessary, eliminate dezinformatsiya. Other projects have also been launched with which the government, military personnel, and the Lithuanian media fight together against dezinformatsiya. Notable is the elves movement, which has led to a hard and grim information war under the guise of a 'seemingly charming fairy tale' starring elves and trolls.

Relevance for the Netherlands

Dutch government organisations and media often feel uncomfortable about far-reaching cooperation projects with the Netherlands armed forces in order to tackle unwelcoming information. On the other hand, to all intents and purposes, the Netherlands government would do well to consider setting up an inter-departmental unit to prevent unwanted interference via all sorts of manipulated information. Let's be honest, in the security domain, the Netherlands suffers from a very serious form of the gullibility syndrome: 'Oh well, it won't happen to us, we are perfectly safe behind the dikes and surrounded by friendly nations, such as Germany, Belgium, France and the United Kingdom.' However, Russian dezinformatsiya campaigns in other countries are a wake-up call for the Netherlands, its society, its government and its institutions. It should be kept in mind that the Netherlands' firm and critical attitude towards Russia's alleged involvement in the MH17 disaster, the support of Dutch government institutions for FBI revelations about Russian hacker groups, [70] the immediate expulsion of Russian security officials following the hack into the OPCW in The Hague, the solidarity with the United Kingdom during the Skripal affair, and Dutch military participation in NATO's eFP in Lithuania, inevitably lead to a Russian response. It is therefore paramount for the entire Dutch society to be well aware of the likelyhood of being targeted, now and in the future, by Russian dezinformatsiya campaigns. ■

70 Huib Modderkolk, 'Dutch Agencies Provide Crucial Intel about Russia's Interference in US-elections', *de Volkskrant*, 25 January 2018. See: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/; Max Smeets, 'The Netherlands just Revealed its Cybercapacity. So What Does That Mean?', *Washington Post*, 8 February 2018. See: https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/.

How to operate in the information environment

A practitioner's perspective from 1 (German/Netherlands) Corps

Information has always been an integral part of conflict. Recent disinformation campaigns brought the information environment to the forefront in military planning and doctrine. How should military units operate in the information environment, how can they become successful in this domain? Experiences gained at 1 (German/Netherlands) Corps show the importance of strategic communication and other information capabilities in an integrated information effort.

*Colonel Dr. Joris van Esch and Colonel Simon Hirst**

'You might not see things yet on the surface, but underground, it's already on fire'

– Indonesian writer Y.B. Mangunwijaya[1]

We all live in a world where the information revolution is widely considered a reality, in a world with a 24/7 news cycle, in which a short video of an arrest causes worldwide demonstrations, or where news, fake-news, and propaganda are an unmistakable part of our language, and in a world where our own actions are judged in an instant. In this world, a great body of knowledge on information has been developed over the years, including a lively discourse on the fragmentation of the infosphere, sensationalism, and its consequences for society. A recent RAND-report, for example, argued that the emergence of multiple technologies like artificial intelligence could change people's fundamental social reality, threatening social coherence and democratic stability.[2]

Throughout the ages, information has also played a key role in conflicts. Clausewitz questioned whether war was to be considered as 'just another form of expression of [the government's] thoughts, another form of speech or writing.'[3] As an example, strategic narratives frame how actions are understood by different audiences, and interweave the trinity of the public, war, and politics.[4] Or the other way around, some even argue that social media have reshaped conflict itself and that it is not about whose army wins, but whose story wins.[5]

* Col dr. Joris van Esch is an officer in the Royal Netherlands Army, and now Deputy Chief of Staff Communication & Engagement at Headquarters 1 (German/Netherlands) Corps, Münster (Germany). Col Simon Hirst is an officer in the British Army, and until September 2020 Assistant Chief of Staff for Information Operations and Targeting in the same headquarters.

1 Naomi Klein, *No Logo: No Space, No Choice, No Jobs* (London: Fourth Estate, 2010) iv.

2 Michael J Mazarr et al., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica, CA, RAND Corporation, 2019) 115.

3 Carl von Clausewitz, *On war*, ed. Michael Howard and Peter Paret (Princeton, N.J., Princeton University Press, 1976), 252.

4 As an example, see the analysis on strategic narratives in the Afghan war in: Beatrice de Graaf, George Dimitriu, and Jens Ringsmose, *Strategic Narratives, Public Opinion and War: Winning Domestic Support for the Afghan War* (Routledge, Abingdon, 2015) 351.

5 David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York, Basic Books, 2017).

Integration of information into military planning is key to operational success PHOTO U.S. AIR NATIONAL GUARD

On the strategic and operational level, the war in Afghanistan clearly showed NATO's deficiencies in the information environment, such as a lack of coordinated and integrated information efforts. It took another conflict to take the next step, and the Russian annexation of Crimea in 2014 was definitely a wake-up call for NATO in that regard. Shortly after the conflict started, NATO's member states realized both the importance of disinformation in Russian doctrine and its effects on their domestic audiences. As a consequence, NATO officially adopted and implemented Strategic Communication, in order to better align strategy, action, and communication.[6]

On the tactical level, one could observe the increase and further development of military information capabilities, such as Psychological Operations. Countries like Germany have even organized similar capacities in a separate command, on the joint level, as another service of the military.[7] Moreover, doctrine has evolved significantly. In the context of conflicts below the threshold for lethal force, NATO has elevated information to a warfighting function, on the same level as Fires, or Command & Control, for example. The U.S. Army did this as well, not only 'to provide the capabilities to influence adversarial actions outside of lethality', but this change intends to 'serve as a catalyst for the required institutional mindset change'.[8] Also in the Netherlands, the joint function information has been introduced into the latest Dutch doctrine.[9]

6 Neil MacFarquhar, 'A Powerful Russian Weapon: The Spread of False Stories', in: *The New York Times*, 28 August 2016. See: https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html; Mark Laity, 'NATO and Strategic Communications', in: *The Three Swords Magazine* 33 (2018) (9).

7 'Kommando Cyber- und Informationsraum'. See: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum.

8 Charles M. Kelly, 'Information on the Twenty-First Century Battlefield Proposing the Army's Seventh Warfighting Function', in: *Military Review* 100 (2020) (1) 66. See: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-20/Kelly-Info-warfighting.pdf.

9 Ministerie van Defensie, *Nederlandse Defensie Doctrine*, February 2019, 90.

PHOTO RIJKSOVERHEID, RICHARD VAN ELFEREN

Some argue that social media have reshaped conflict itself and that it is not about whose army wins, but whose story wins

Now celebrating its 25th anniversary since its founding, 1 (German/Netherlands) Corps (1GNC) based in the German city of Münster, is one of NATO's High Readiness Force (Land) Headquarters. It is able to deploy as a Corps Warfighting Headquarters, as NATO Response Force Land Component Command, or as Joint Task Force (Land) Headquarters. In addition, 1GNC acts as a professional training platform for divisions and brigades.[10] Within this context, 1GNC has developed its understanding on how to deal with the joint function information. As the authors both have been working on the information environment within 1GNC, they thought it timely to pass on what they had observed and learnt. To develop its ideas and concepts, 1GNC has experimented, learnt, and implemented Strategic Communication in its organisation and battle rhythm. The authors believe their headquarters (HQ) is in a favourable position to further develop information, given 1GNC has a breadth of expertise, staff capacity and experience with all information capabilities, and is continuously adapting its approach and procedures in the information environment. This is mirrored in the organisational structure itself, where the importance of the non-lethal environment is integrated and apparent from the outset of planning and subsequent execution.

The central argument in this article is that the key to operational success (and especially in the information environment), on the tactical, operational, and strategic levels, entails a seamless and successful integration of information into military planning and application of operational art. As far as is possible within

10 For more information on 1GNC, see https://1gnc.org.

the context of a public article, strengths, weaknesses, and opportunities will be described. Subsequently, it will be discussed how 1GNC deals with the joint function information, including targeting, and how this played out during various exercises. To conclude, the authors will offer some reflections on what they have experienced over the last few years. However, as the doctrine and thinking about information in the military realm still suffer from a lack of broad common understanding, the article starts with providing some basic definitions of NATO's activities, capabilities and effectors in this domain (see Table 1).

Table 1 Overview of definitions of NATO's communication activities and capabilities[11]

Public Diplomacy: NATO civilian communication and outreach efforts responsible for promoting awareness of and building understanding and support for NATO's policies, operations and activities, in complement to the national efforts of Allies
Public Affairs: NATO civilian engagement through the media to inform the public of NATO policies, operations and activities in a timely, accurate, responsive, and proactive manner
Military Public Affairs (PA): promoting NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance
Information Operations (IO): NATO military advice and coordination of military information activities in order to create desired effects on the will, understanding, and capabilities of adversaries and other NAC-approved parties in support of Alliance operations, missions and objectives
Psychological Operations (PsyOps): planned psychological activities using methods of communication and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives
StratCom, in the context of the NATO military, is the integration of communication capabilities and information staff functions with other military activities, in order to understand and shape the Information Environment, in support of NATO aims and objectives

Information within 1GNC

NATO doctrine provides us with a common philosophy, a common language, a common purpose, and a unity of effort, whilst Standard Operating Instructions provide further guidance. The key is that 1GNC's headquarters structure follows NATO's latest Military Policy on Strategic Communications (StratCom).[12] This policy sees StratCom moving from a purely advisory and coordination function, to that of holding the Commander's delegated authority. StratCom in NATO is a command responsibility that spans all levels. It directs, coordinates, and synchronizes the overall communication effort and ensures coherence across the communication capabilities and information staff functions. This is often referred to as the 'Golden Thread'.

In 1GNC, staff officers for StratCom, Information Operations (including Key Leader Engagement), Targeting, Electronic Warfare, PsyOps, and Military Public Affairs) are all grouped in one of the four divisions of the HQ, under a Deputy Chief of Staff for Communication and Engagement. This ensures their integration within the HQ's operations analysis, planning, execution and assessment, in accordance with the commander's intent and objectives. In contrast with NATO's StratCom Policy, the Communication & Engagement division also includes the CIMIC (G9/J9) Branch. Experience has demonstrated that this ensures a comprehensive approach in all operations; a crucial perspective embedded in the DNA of 1GNC.[13]

11 These definitions are shorter than (but similar to) definitions from official NATO doctrine: 'About Strategic Communications'. See: https://www.stratcomcoe.org/about-strategic-communications. The StratCom definition is derived from NATO MC0628. NATO Military Committee, 'NATO Military Policy on Strategic Communications (MC0628)', 14 August 2017. See: http://stratcom.nuou.org.ua/wp-content/uploads/2020/01/NATO-MILITARY-POLICY-ON-STRATEGIC-COMMUNICATIONS.pdf. For official definitions, see the latest (respective) NATO doctrine documents.

12 NATO MC0628.

13 In addition, a senior official of the Dutch Ministry of Foreign Affairs is seconded to 1GNC, to advise on the civil and political aspects of an operation from a foreign policy and human security perspective.

The authors found that this organisational structure and grouping of several of these disciplines, including CIMIC, has generated a deeper understanding, more resilience, and better cross functional cooperation, both in the planning and execution of operations.[14] Notably often only a higher tactical level like 1GNC has this breadth of expertise and capacity, with a few dozen different staff officers from various backgrounds; while divisions and brigades usually have limited means and capabilities to deal with challenges in the information environment. The high turnover of staff and specific subject matter expertise is, however, a training and continuity challenge, sometimes shared with other NATO staffs. But the nucleus remains sound, robust and fit for purpose.

Recent experiences with the information environment

It appears that there is never any shortage of direction and guidance from the strategic and operational levels on the 'What' and 'Why' of an operation, but focus at the tactical level also has to be on the 'How?', in order to achieve the Commander's objectives. In essence, this is what Mission Command is all about. To quote a previous Commander of 1GNC, who at STARTEX was prone to say: 'show me what you are doing, where are the actual products and make it tangible'. The last few years have provided realistic opportunities to the Professional Training Platform to conduct academics, Battle Staff Training and to test procedures at the German Army Warfighting Centre in Wildflecken and, of course, to make it tangible.

PHOTO 1GNC

1GNC's Public Affairs officers participate in an exercise

1GNC has refined its contributions during Crisis Response Planning with relevant input to operational plans and orders. Coupled with this has been the imaginative scripting of an enemy modus operandi that incorporates an effective Influence Campaign that demands a response from the military and others, in order to develop a common mindset that views the information environment as being inextricably linked to the physical environment.

The Corps' training audiences have not been virtual or abstract. Tempo, friction, fatigue, and pressure have often felt very real. There has been plenty of scope for 'testing and adjusting' within the HQs of 1 (DEU) Armoured Division and (DEU) Rapid Forces Division during Exercise Vital Sword in 2017. This also included many other multinational secondary training audiences and response cells, such as 11 (NLD) Air Manoeuvre Brigade and 43 (NLD) Mechanised Brigade. Further, as 1GNC was in the lead for the certification of the NRF 19 VJTF (L) Brigade (based on the 9 (DEU) Lehr Brigade in 2018), tangible progress could be measured.

1 (DEU) Armoured Division was once again put through its paces in 2019, during Exercise Xenon Sword, together with 13 (NLD) Light Brigade and 1 (NOR) Brigade North. Within the Area of Operations they were faced with hybrid threats and an unfolding humanitarian crisis that threatened to impact the operation. Examples include a displaced population clogging up lines of communication, the lack of basic needs for the civilian populace, and the enemy's use of

14 In line with the MC0628, Chief PA (the spokesperson) retains its independent advisory role and direct access to the Commander on Public Affairs matters.

propaganda on exercise social media accounts, where the training audiences' actions or indeed perceived mistakes and actions could be exploited. Throughout the build-up of the exercises, and detailed in the After Action Reviews, commanders at all levels displayed an increasingly firm grasp of the complexity and utility of the information environment. The blurring of the lines between war and peace and an enemy not following a familiar template were met with recognition and involvement of the Public Affairs Officer and Key Leader Engagement from the outset, with support from PsyOps, CIMIC, Electronic Warfare and other subject-matter experts, allowing commanders to incorporate many non-lethal effects in their planning and execution.

When combined in a Comprehensive Approach, commanders could tackle the complex scenarios and recognise that at the tactical level the preponderance of communication is achieved by what is actually done — rather than by what is said. However, the value of using 'traditional' messaging techniques, such as leaflet drops and radio broadcasts etcetera was also not dismissed, especially in those areas where civilian infrastructure was lacking. Many of the PsyOps products also proved the complexity of the information environment. To understand what it would take to defeat the enemy's will to fight requires a thorough Target Audience Analysis.

Targeting

Targeting is a process of determining the effects necessary to achieve the commander's objectives, and of identifying the actions necessary to create the desired effects based on means available. Furthermore, the process includes selecting and prioritising targets, synchronising fires with other military capabilities, and then assessing their cumulative effectiveness and taking remedial action, if necessary.[15] To many, this conjures up an image of precision-guided munitions being delivered onto targets from various platforms.

However, in every operation one must also be able to influence adversaries, the local population, or even attack enemy information capabilities and to protect one's own information capabilities to affect enemy understanding. This realisation that being able to combine lethal and non-lethal effects with kinetic and non-kinetic means in the targeting process requires the right mindset and is often challenging for all members of the staff to understand.

Key in the approach of 1GNC is that its targeting process is aimed at achieving effects in all domains and all battlespaces, and integrates both lethal and non-lethal targeting in one and the same process. In this context, in 1GNC communication is often referred to as a 'weaponeering' solution. What has been observed is that this works well at Joint and Corps level, and incorporates target nominations at the Divisional and Brigade levels.

This implies that a number of Working Groups in the 1GNC Battle Rhythm leads to an Information Operations and Targeting Coordination Board, where timely decision-making on synchronisation of effects and means have helped in its conceptual development. The Target Approval process, like much else, requires practice and an understanding of the level at which delegations are held and where assets and expertise external to an HQ can play a role in the process through Liaison Officers. Many may also be struggling with the concept that a large number of the desired effects often require extensive planning. Moreover, it could also last many months before the effects of a messaging campaign could be observed in the behaviour of the local population.

Experiences in Norway – Exercise Trident Juncture

An opportunity for putting into practice what had been learnt and conducting further experiments was the introduction to, preparation for,

15 *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*, 2016.

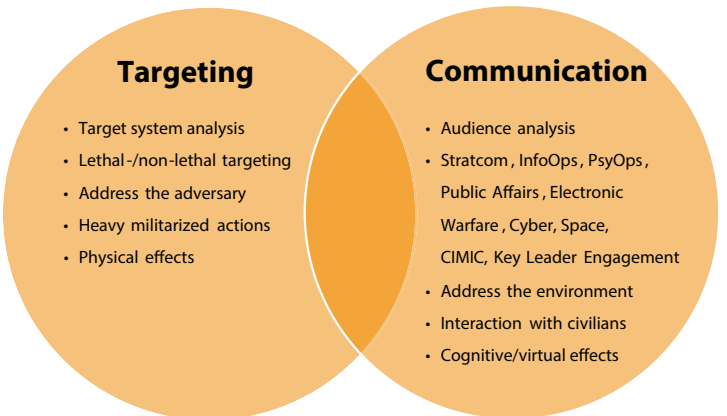


Figure 1 1GNC's approach to targeting: integration of both lethal and non-lethal targeting in one process

and delivery of Exercise Trident Juncture in 2018. This NATO-exercise in Norway included 50,000 participants, 250 aircraft, 10,000 vehicles, and 65 vessels from 30 nations. It was also a significant opportunity to be fully exploited for real-life StratCom effect in support of NATO objectives. An Integrated Communication Plan provided coherence with a focused 'whole of NATO' effort.

StratCom synchronisation was required both horizontally within the HQ, as well as vertically to ensure message coherence and to create a Golden Thread from the political/strategic to the lowest tactical level. To busy multinational staff officers, StratCom Frameworks with their key messages and narratives could be challenging to absorb at first sight. They required a healthy dose of distillation in order to be fully understood and implemented. The practice of summarising the essence of the frameworks was outlined on simple Participant Cards containing facts, such as troop numbers. However, in a dispersed command structure and in a multinational setting it was not always easy to exploit every phase of the exercise. Preparation, from Reception Staging and Onward Movement to Integration activity, should not be overlooked. The requirement, therefore, during Commanders' conferences to confirm the StratCom Golden Thread must always be briefed. The Golden Thread provided a clear understanding of what NATO was trying to achieve, allowing for both a vertical and horizontal alignment at all levels of command. The requirement for operational security was also discussed in detail and practised. One such aspect are soldiers' actions on social media and reliance on personal electronic devices. To assist in this education there are several good national examples that provide direction and guidance for the use of social media that have helped to shape behaviour and recognise the advantages and disadvantages of its use during operations and peacetime activities.

This exercise also exposed the limitations of conducting assessments of actions within the setting and relatively short duration of the CPX phase. Joint Targeting Coordination Boards with higher HQs and other Component Commands certainly synchronised the lethal and non-lethal effects. The resultant Battle Damage Assessments and Measurements of Effectiveness of a Deception Operation, which included radio messages, exercise social media, and leaflets to encourage enemy forces to surrender, for example, requires dynamic scripting to complete the Cycle and provide realistic feedback for the ensuing planning.

It also became clear that 1GNC's own information activities caught the attention of the Joint Force Commander. Delegation of authorities such as Target Engagement and PsyOps Product Approval, which were thought to be clear from the outset, still created a healthy discussion concerning at what level they should be held, given that the effect of a dropped leaflet could outlast the impact of dropping a bomb.

In this exercise, the cooperation and the reach back capacities of the German *Bundeswehr's Zentrum Operative Kommunikation* in Mayen proved to be very valuable. Recognition of their capabilities and experience coupled with frequent visits developed a fruitful exchange of ideas and techniques that could be applied in the form of sophisticated visual and audio products designed to degrade the will of NATO's potential opponents.

The conundrum of operating in an exercise setting, whilst also cognisant of 'real-life' perception management, and profile and posture in the host country Norway (which was also very attuned to a real battle of the narratives), was instructive for NATO's deterrence and reassurance measures.

The NATO Media and Information Centre, augmented with members of 1GNC PA, was well-resourced and prepared for its task. Media training prior to deployment was conducted, but perhaps this could have focussed on a wider cross-section of the staff to allow more junior officers and NCOs to tell their stories. After all, everyone is a communicator. The Norwegian Ministry of Defence provided daily reports throughout the exercise on how the exercise was perceived amongst the population over time, and was able to provide a genuinely positive measurement of effectiveness. The successful Distinguished Visitors Day near Trondheim sent a clear political message of NATO's cohesion, whilst Sputnik and RT stories provided the predictable counter narrative. There were some good examples of this, but timely counter-messaging at the highest level with the intention to be the first out with the truth, and dispel fake news about where NATO-troops were exercising, troop numbers, the intent with the 'Golden Thread', and NATO's cohesion underpinning this effort.

How to bring the outside world in?

1GNC has recognised and learnt that exercising in the information environment does not begin and end at the gates of Wildflecken, or when undergoing its own certification. In contrast with crisis response operations, which are limited in time and space, the information environment is omnipresent. In 1GNC, it is also considered 'in peacetime' how to assist in helping to shape the attitudes and behaviours of intended audiences. Instructive questions used were, for example, 'How do we see ourselves and through what lens do external actors and audiences that matter most to us see us?' And 'how do we bring the outside world in?' This sounds obvious, but some of us live in an information 'comfort bubble', often termed by

NATO exercise Trident Juncture provided opportunities to practice what had been learnt PHOTO NATO

Many of us are often oblivious to the negative and subtle narratives being played out against us over time

others as the 'echo chamber'. Many of us are often oblivious to the negative and subtle narratives being played out against us over time and the fact that objective facts are often less influential in shaping opinion that appeals to people's emotions and personal beliefs.

In order to tackle this perceived lack of perception, 1GNC formed a peacetime Information Activities Working Group. It seeks to generate an information environment awareness across the staff, synchronise ideas, reflect on previous activity and look ahead to how 1GNC can improve and harness key events and activities that can create information effects. This should also build resilience and make the most of 1GNC's reach on social media and through other outlets, whilst benefitting from a more nuanced analysis that seeks to send the message to the right audiences. Perhaps a good measure of effectiveness also includes how friends and families talk about what we all do?

The next steps, as 1GNC prepares for JTF HQ (L) certification in 2020 and its role as PTP for 10 (DEU) Armoured Division in 2021, will, however, include improving understanding of what is already available through Open Source, the NATO Multimedia library, national examples and regular communication with Centres of Excellence. The staff must continuously be sensitised to the importance of the information environment with the opportunities and threats it presents.

Reflection

In this article, the authors have shared their perspective on the information environment: how to understand it, how to synchronize information capabilities, and how to operate in this environment. Based on their experiences, these are some of their insights and reflections.

First, it must be stressed that any planning and execution in the information environment requires a thorough understanding and analysis of the specific and relevant information environment. Often, evidently these analyses are limited to what is currently happening, not continuously, restricted to the Western perspective, and limited to media-, web- and social media-monitoring. This is reinforced by the abundance and speed of information. However, in order to be successful, synthesis is paramount. What are the trends, and what do they mean? How does information affect attitude and behavioural patterns of different audiences? And where does this offer opportunities (and threats), especially at our level, and within our means and capabilities to act in the information environment? We have learnt that this depth of analysis, followed by deliberate planning and coordination, requires a significant amount of time, expertise and effort, which is not always available.

Over the years, the personnel at 1GNC have developed a mindset that enables leaders and staff to understand the information environment in the broadest sense, and train, plan, and act accordingly. This change took years, both practically and culturally. In hindsight, a prerequisite is a strong, professional force of specialists in the different communication disciplines. We were fortunate to work with these individuals and teams. However, they have usually received training or gained experience in only one of the career fields. Oversight does require insight; and building up the required level of expertise will require more experience on different levels and in different fields.

Relatedly, it does not help that this relatively new field of expertise suffers from an

'How do we see ourselves and through what lens do external actors and audiences see us?' PHOTO U.S. AIR NATIONAL GUARD

abundance of unclear, overlapping, or even a conflicting body of knowledge. The continuous development and implementation of new terms, and the conceptual nature of this field, does contribute to a lack of common understanding, both within the information-related disciplines and, more importantly, with other fields of expertise and senior leadership. New doctrine, like the upcoming NATO doctrine on StratCom will assist, but the military definitely needs a simplification of the terms, to make 'outsiders' better understand how to integrate information as a joint function into warfighting. In this context, the Dutch military could be clearer on its emerging concept of Information Manoeuvre as well; how and where does it add which relevant operational value and where does it overlap with the existing capacities, capabilities, and doctrine. The Dutch are not alone in this regard; a recent RUSI report, for example, argued that also the British Army should become more comfortable with working outside the purely military space, and with blending non-kinetic capabilities and effects with already existing and well-developed kinetic effects and capabilities.[16]

Conclusion

This article is built on experiences gained at 1GNC with others and shows that probably a key factor for successful operations is the amalgamation of information with other joint functions. In the crisis response planning phase of an operation, StratCom and other information capabilities planners should be involved in developing courses of action with the most advantageous likely outcomes. Becoming successful in the information environment is definitely not about 'sprinkling information effects' onto an existing plan. In the execution phase, it was found that Joint Targeting has proven to be most effective to synchronize actions and effects in *all* domains. Therefore, in a world where conflicts abound and where perceptions become reality, the key to operational success on the tactical, operational, and strategic levels is successful integration of information into military planning and application of operational art. ■

16 Nick Reynolds, 'Performing Information Manoeuvre Through Persistent Engagement', *RUSI Occasional Paper*, June 2020, 54. See: https://rusi.org/sites/default/files/20200611_reynolds_final_web.pdf.

Identiteitscrisis: 'Ik denk, dus ik ben'

Hoe onze denkfouten de doorontwikkeling van de krijgsmacht belemmeren

De veranderende karakteristieken van conflict en de toenemende complexiteit van onze omgeving stellen nieuwe eisen aan de krijgsmacht. We moeten ons continu aanpassen om relevant en slagvaardig te blijven. De huidige veranderingen betekenen misschien wel de noodzaak voor een paradigmaverschuiving in ons denken over conflict, in ons beeld van slagkracht en zelfs in de invulling van militaire identiteit en leiderschap. Het vergt echter durf en mentale lenigheid om onze geconstrueerde 'waarheden' over conflict, slagkracht, identiteit en leiderschap ter discussie te stellen.

*Kapitein-luitenant ter zee Roel Samson en luitenant-kolonel Gwenda Nielen**

Het is gemakkelijker gezegd dan gedaan. Objectief redeneren is voor een mens namelijk onmogelijk. Dat komt doordat er verschillende systematische vertekeningen, zogenoemde cognitieve *biases*, in ons denken zitten.[1] Zelfs wij, zelfverklaarde rationele denkers, redeneren in meer of mindere mate in de richting van conclusies die wij als waarheid of feit beschouwen en die passen binnen de culturele en sociale context waarin we acteren. Het beïnvloedt hoe en welke informatie we verzamelen, interpreteren en verwerken, wat we ons uit het verleden herinneren en dus ook hoe we de werkelijkheid waarnemen en interpreteren. Hoewel er lezers zullen zijn die dit essay als een persoonlijke aanval zullen ervaren, is het bedoeld als een *eye-opener* naar mechanismen in ons menselijk denken en processen in onze organisatie die er toe leiden dat we niet objectief en rationeel (kunnen) denken en handelen. Het kritisch reflecteren op systeemproblemen in ons denken en doen die verankerd zijn in onze organisatie, militaire cultuur en identiteit is de eerste stap in het beperken van het negatieve effect van deze 'normale', maar ongewenste fenomenen op de keuzes die we maken.

Hoe cognitieve biases ons denken en doen beïnvloeden komt naar voren in de manier waarop ons beeld van moderne dreiging en conflict wordt geconstrueerd en wat dat betekent voor de rol, taak en samenstelling van de krijgsmacht.

Dreiging en conflict

Niet zo lang geleden was de wereld voor de militaire denker relatief overzichtelijk. De leidende wereldbeelden van kapitalisten en communisten stonden lijnrecht tegenover elkaar en alleen fysiek overwicht kon de ander van mening doen veranderen. De opbouw van een nucleair arsenaal dat uiteindelijk leidde tot een patstelling die passend MAD (*mutual assured*

* Roel Samson is werkzaam bij de staf van het Defensie Cyber Commando. Gwenda Nielen werkt bij de Counter Hybrid Unit van het Directoraat-Generaal Beleid. Dit essay is geschreven op persoonlijke titel.

1 Biases die ons belemmeren objectief te kunnen zijn, zijn onder meer: cognitieve dissonantie, *confirmation bias*, *groupthink*, *consistency*, *self-serving bias*, Dunning-Kruger-effect, *empathy gap*, *loss aversion*, *mere exposure effect*, *overconfidence effect* en de Semmelweis-reflex.

FOTO US CENTRAL INTELLIGENCE AGENCY

We moeten open minded naar de wereld kijken om weerstand te kunnen bieden aan de neiging het 'oude' conflict te kopiëren naar ons beeld van de toekomst

destruction) genoemd werd, kan ook in dat kader worden gezien. De Berlijnse Muur viel en langzaam maar zeker werd duidelijk dat de fysieke Russische legers niet zo formidabel waren als gedacht. De NAVO had na de Koude Oorlog een korte periode van suprematie, hoofdzakelijk gebaseerd op fysieke militaire superieure systemen. Maar onze opponenten hebben, zoals ook de strategische denker en professor David Kilcullen schrijft, veel effectievere manieren gevonden om hun belangen te behartigen dan het gebruik van militaire slagkracht in de fysieke dimensie.[2]

Tegenwoordig zetten statelijke en niet-statelijke actoren georkestreerd al hun machtsmiddelen in om hun belangen te behartigen ten koste van die van andere staten, de EU, of de NAVO. Deze actoren hebben een grondige analyse gemaakt van de kwetsbaarheden van westerse systemen en weten dit uit te buiten. Het militaire machtsmiddel van lethale confrontatie is daarbij een *last resort*-strategie geworden. De heersende gedachte is juist om gewapende militaire confrontaties te vermijden: de kosten ervan zijn enorm en wegen eigenlijk nooit op tegen de baten. Daarnaast is het wenselijk om onder de grens van 'juridisch oorlogvoeren' te blijven en beïnvloeding van burgers in te zetten, zodat westerse legers tandeloze tijgers blijven in een hermetisch afgesloten box van juridische beperkingen en negatieve publieke opinie. Precies deze twee aspecten, die wij als democratische staten zwaar laten meewegen in onze besluitvorming, zijn voor onze opponenten haast irrelevant.

2 David Kilcullen, *The Dragons and the Snakes. How the Rest Learned to Fight the West* (Londen, Hurst, 2020).

Op basis van de bovenstaande observaties zouden we met rationele en realistische argumenten toch tot de conclusie moeten komen dat we, naast het doorontwikkelen van mogelijkheden in de fysieke dimensie, nu vooral ook moeten investeren in slagkracht, weerbaarheid en afschrikking in de virtuele én cognitieve dimensie. Hoewel we het al jaren opschrijven in visiedocumenten en beleidsstukken, wordt het niet gedragen in de organisatie of vertaald in de defensieplannen en uitgaven. We zullen daarom meer moeten investeren in een breed militair-strategisch denkvermogen, zodat de visie ook wordt omgezet in daadwerkelijke veranderingen in de organisatie. Dit denkvermogen rondom een modern conflict zou centraal moeten staan; niet alleen binnen het ministerie van Defensie, maar gezien de huidige dreiging ook inter-departementaal. We willen niet verworden tot de dinosaurus van 21e eeuw: groot en in potentie fysiek sterk, maar zonder een goed ontwikkeld strategisch brein en capaciteiten om reële dreigingen het hoofd te bieden.

De realiteit

Waarom blijven we dan toch vooral investeren in capaciteiten die we nodig hebben voor een gewapend militair conflict, waarin we vechten in een hoog geweldsspectrum tegen een *near-peer competitor*? Een gevecht waarin militaire opponenten tegenover elkaar staan en elkaar met vuurkracht bestrijden; een gevecht zoals we dat kennen uit films en *battlefield tours*? En dat terwijl we ons midden in het scenario bevinden waarin staten alle machtsmiddelen benutten om 'ons' uit te manoeuvreren.[3] In het eerste gevecht zijn de burgers slachtoffer of een factor in de operationele omgeving, maar in de benadering van onze belangrijkste opponenten zijn zij spelers, misschien wel de belangrijkste spelers op het veld.

Waarom houden we als defensieorganisatie dan vast aan een irreëel scenario? Wellicht heeft dat te maken met het beeld dat we hebben geconstrueerd van een krijgsmacht die als *last line of defence* dient om onze maatschappij fysiek te verdedigen tegen invasies door 'vijandelijke' staten, in plaats van een organisatie die een belangrijke rol speelt in preventie van mogelijke brandhaarden, verdediging van nationale belangen en de-escalatie van conflicten en daarvoor overduidelijk meer moet kunnen dan alleen het fysieke verdedigen van grondgebied. Mensen houden van nature niet van complexiteit.

Beeld van conflict

Om *open minded* naar de wereld te kijken en weerstand te kunnen bieden aan de neiging het 'oude' conflict te kopiëren naar ons beeld van de toekomst, moeten we eerst de terminologie rondom conflict ontrafelen. Zoals gezegd hebben wij onze organisatie grotendeels gemodelleerd rondom een beeld van grootschalig conflict in het hoge geweldsspectrum tegen een near-peer competitor. Deze omschrijving is echter slechts passend voor een zeer beperkt aantal oorlogen in de laatste eeuwen en heeft als belangrijkste kenmerk dat we van tevoren niet zeker weten of we deze kunnen winnen. Als we dit in perspectief zien was de laatste oorlog die hieraan voldeed de Tweede Wereldoorlog en zelfs toen was de zaak pas beklonken op het moment dat de VS door Japan in het strijdgewoel werd betrokken. *Let's face it*: geen militair die op dit moment in actieve dienst is heeft ooit een dergelijk conflict meegemaakt. Het is des te meer bijzonder dat een oorlog die niemand binnen de huidige krijgsmacht heeft gevochten, model staat voor het kader waaraan we ons spiegelen. De focus ligt daarbij voornamelijk op materieel en de modernisering ervan. Dat is het onderdeel van militair vermogen dat de toets moet kunnen doorstaan van grootschalig conflict. We verliezen uit het oog dat de Tweede Wereldoorlog vooral grootschalig was op het gebied van aantallen manschappen. Miljoenen jonge mannen streden in dit grootschalige conflict vaak te voet en op cruciale momenten waren er niet per definitie vliegtuigen of tanks betrokken.

In het brein van de meeste militaire denkers na 1950 ontstond het beeld van de *all-out war*. De dreiging is een combinatie geworden van de

3 Dit betekent de strategische en opportunistische inzet van een combinatie van diplomatieke, informatie-, militaire, economische, sociale en juridische (Lawfare) machtsmiddelen.

schaal van de Tweede Wereldoorlog met de *doomsday*-toevoeging van technologische ontwikkelingen en nucleaire wapens. Geen wonder dat de dreiging van deze potentiële atoomoorlog ook nog impact heeft op het huidige denken over conflict. Want hoewel de illusie van een onvermijdelijke Derde Wereldoorlog is weggenomen, verdween dit angstig makend oorlogsbeeld nooit echt uit onze organisatie. Sean McFate beschrijft in zijn boek *Goliath* heel pakkend hoe we vastzitten in een verkeerd beeld van het moderne conflict omdat we het baseren op ons beeld van het verleden met daaroverheen een laagje technologie en science fiction.[4] Logisch ook, want het zelfbeeld van wat een militair moet zijn en kunnen is al die jaren ontleend aan grootschalige conflicten met confrontaties in de fysieke dimensie.

FOTO DARPA

Volgens Sean McFate baseren we ons beeld van het moderne conflict op het verleden met daaroverheen een laagje technologie en science fiction

In het huidige internationaal-politieke theater zijn de militaire verhoudingen uit de Koude Oorlog niet fundamenteel gewijzigd; nog altijd heeft de NAVO een substantieel militair voordeel ten opzichte van Rusland. President Poetin weet dit als geen ander, maar hij kent vooral ook de zwakheden van onze alliantie: het onvermogen om buiten de kaders van 'formele' oorlog op te kunnen treden, een nadruk op de militaire component van conflict en de fysieke dimensie, een beperkte interdepartementale samenwerking binnen de onafhankelijke staten en de complexe cohesie binnen de NAVO.

Waarom het pijn doet...

Voor veel militairen is militair zijn geen beroep, maar een belangrijk onderdeel van de identiteit. En omdat veel militairen de defensieorganisatie hebben geïnternaliseerd staat het ter discussie stellen van het heersende beeld van conflict of de relevantie van de krijgsmacht gelijk aan het ter discussie stellen van het bestaansrecht van de militair zelf. Identiteit is een emotioneel beladen onderwerp. Het is de basis van wie we (denken te) zijn en alle zaken die de identiteit bedreigen resulteren in weerstand, ontkenning of zelfs agressief handelen. Dat hebben we gezien in maatschappelijke discussies over bijvoorbeeld het stemrecht voor vrouwen, dat de identiteit van de man als autoriteit en de vrouw als gehoorzaam aantastte. Maar ook bij het homohuwelijk, wat de identiteit van echtgenote of echtgenoot veranderde. En denk ook aan de binnenkort weer opspelende discussie rondom Zwarte Piet. Zijn zwarte kleur is volgens sommigen zo cruciaal voor het Nederlanderschap dat deze niet met roetvegen of in een regenboogversie wordt geaccepteerd. Het is duidelijk dat er bij fundamentele veranderingen die de identiteit raken altijd weerstand is. Het zou dan ook een illusie zijn om te verwachten dat militairen hun door de historie heen zorgvuldig opgebouwde identiteit zonder slag of stoot zouden willen of kunnen veranderen. Maar de weerstand gaat dieper, want we hebben niet alleen een verdraaid beeld van conflict, maar ook van de mensheid als geheel.

Bij de meeste organisaties die hun bestaansrecht ontlenen aan de donkere kant van de mensheid (zoals de politie en de krijgsmacht) is de identiteit gestoeld op een negatief mensbeeld, zoals beschreven door de Engelse filosoof Hobbes.[5] Veel collega's geloven sterk in de

4 Sean McFate, *Goliath: Why the West isn't winning. And what we must do about it* (Londen, Penguin, 2019).

5 Thomas Hobbes, *Leviathan or the Matter, Forme and Power of a Commonwealth Ecclesiastical and Civil* (orig. 1651) (geredigeerd met introductie: Londen, Penguin, 2017).

FOTO MCD, JARNO KRAAYVANGER

stelling dat de mens maar een dun laagje beschaving heeft en dat hij, als dit verdwijnt, steevast verandert in een beestachtig wezen. De identiteit van de militair kenmerkt zich door zinsnedes als: 'wij zijn de laatste optie en wij zijn bereid om te doen wat nodig is als ons land bedreigd wordt'. Deze haast fatalistische benadering vindt in de recente geschiedenis genoeg grond om breed geaccepteerd te worden. De generatie opa's en oma's maakte de oorlog nog mee en de babyboomers erna werden door de verhalen haast meegenomen naar de jaren 40-45. Deze generatie groeide vervolgens op in een periode van Koude Oorlog, waarin Flower Power het moest opnemen tegen de voortdurende dreiging van een nucleair armageddon. Werd je daarentegen geboren in de jaren 80-90, dan nam de dreiging vanuit het Oosten af, maar werd de intensiteit van de menselijke gruwelbeelden steeds sterker. Live-televisie vanuit Bagdad, de misstanden in Mogadishu, en Nederlandse VN-militairen die Srebrenica moeten opgeven. Dit alles cumuleert dan in de 21e eeuw, die wordt ingeluid met *9/11* en de terreuraanslagen van Islamitische Staat.

Mensen die het als hun levenstaak zien de wereld te zuiveren van al dit kwaad en die hun identiteit ontlenen aan het vormen van het tegenwicht voor de duistere kant van de mens, denken slechts zelden in nuance. Wie dat wel doet is journalist en schrijver Rutger Bregman. In zijn boek *De meeste mensen deugen* pelt hij laag voor laag onze menselijke psyche af en maakt korte metten met een heleboel hardnekkige misverstanden. De belangrijkste hiervan is de 'vernistheorie'.[6] Met een breed scala aan voorbeelden onderbouwt Bregman dat de mens zich niet automatisch beestachtig gaat gedragen zodra de beschaving wegvalt. In legio voorbeelden put hij uit onderzoek naar militairen en juist daarom is dit artikel geschreven, want Bregmans onderzoek geeft aanzet tot het onvermijdelijke: we moeten als militairen onszelf opnieuw leren kennen in een wereld die niet overzichtelijk zwart-wit is, maar supercomplex met intergerelateerde problematieken en meer schakeringen grijs dan we ooit voor mogelijk hielden.

Complexiteit versus zekerheid

We leven als militairen in een onmogelijke tijd. De ene paradox is nog sterker dan de andere en om het nog ingewikkelder te maken ligt het defensieapparaat vrijwel permanent onder een vergrootglas van de politiek en de maatschappij. De omgeving waarin we acteren is ingewikkelder dan ooit, terwijl de bij elke militair steevast ontwikkelde kerncompetenties daadkracht en doorzettingsvermogen ons niet helpen om het geduld en de tijd op te brengen om de complexiteit te leren begrijpen. Twijfel, zich kwetsbaar opstellen of terugkomen op eerder genomen besluiten worden gezien als ontwikkelpunten in plaats van als talent. Het is daarom logisch dat militairen in een steeds complexere wereld houvast zoeken in begrijpelijke en overzichtelijke representaties van de *wicked* werkelijkheid en in beelden van de wereld zoals die was, de organisatie zoals je hem kende en de kennis

6 Rutger Bregman, *De meeste mensen deugen. Een nieuwe geschiedenis van de mens* (Amsterdam, De Correspondent, 2019) 25.

Militair optreden houdt tegenwoordig meer in dan klassieke manoeuvre en vindt deels plaats in de digitale en cognitieve dimensies; talent moet alle kans krijgen om zich daarvoor te ontwikkelen

die je ooit hebt opgedaan. Het zijn allemaal ankerpunten in een onzekere wereld. De Russische oorlogswals is niet langer een bedreiging, maar vormt wel een ankerpunt voor een overzichtelijk twee-actorenbeeld van conflict en onze identiteit als vechters. We kunnen door op die manier te denken de nuance en risico's van onduidelijke crisisbeheersingsoperaties en complexe hybride dreigingen achter ons laten in de overtuiging dat het Koude Oorlogsspook nog rondwaart.

Wij als krijgsmacht richten ons op een oorlog van militairen die met tastbare, lethale wapens vechten tegen de combattanten van de opponent en zien oorlog bijvoorbeeld niet in de vorm van hulpgoederen en beademingsapparatuur. Wij (h)erkennen de Chinese militaire hulp aan de Balkan tijdens de Covid-19-uitbraak niet als agressie of oorlogshandeling en als krijgsmacht sluiten we daarmee uit dat er voor ons een rol is weggelegd in de conflicten van vandaag (en morgen). En dit terwijl deze hulp een zeer doelgericht en beoogd effect genereert: het ondermijnt het vertrouwen van de Serviërs in Europa en effent het pad voor meer Chinese invloed. En zo, terwijl statelijke actoren ons van alle kanten uitmanoeuvreren, richten wij ons op het militaire Russische spook dat we kennen en denken te begrijpen. Dat we meer bezig zijn met de historie dan met de toekomst is geïnstitutionaliseerd.[7] En in de op het verleden gefocuste *mindfuck* benadrukken we vooral dat wat ons zelfbeeld bevestigt. Bij de blitzkrieg kijken we dan bijvoorbeeld naar tanks die over de hoogvlaktes manoeuvreerden, terwijl blitzkrieg voor het overgrote deel Information Manoeuvre was,

7 Zie ook: Leon Festinger, *A Theory of Cognitive Dissonance* (Stanford, Stanford University Press, 1957). Festinger geeft aan dat mensen inconsistentie tussen gedrag en geloof of attitude als onprettig ervaren, en daarom gemotiveerd zijn om gedrag en geloof in overeenstemming met elkaar te brengen.

We negeren signalen die ons vertellen dat we misschien wel radicaal moeten veranderen om relevant te blijven

gericht op de cognitieve dimensie.[8] En zo blijven we als militairen volhouden dat het grootschalige conflict in het hoogste geweldsspectrum tegen een near-peer competitor het uitgangspunt zou moeten zijn bij de 'door'-ontwikkeling van de krijgsmacht. Met andere woorden: we creëren het conflict in ons hoofd dat het beste past bij wie we zijn, omdat de realiteit van de huidige dreiging niet langer aansluit bij wie we zijn.

Perspectief voor de toekomst

Moderne conflicten worden tegenwoordig vooral uitgevochten in de digitale en cognitieve dimensies en zijn geen openlijke militaire confrontaties. Onze opponenten richten zich namelijk volgens goed militair gebruik op onze zwaktes. Tegelijkertijd staren wij ons blind op het gevecht dat we denken te kennen en negeren signalen die ons vertellen dat we misschien wel radicaal moeten veranderen om relevant te blijven. We worstelen overduidelijk met onze eigen biases en het referentiekader waarbinnen we zijn opgevoed en negeren daarbij de logische conclusies die we moeten verbinden aan de analyse van onze opponenten: oorlogvoering in de 21e eeuw ziet er fundamenteel anders uit dan voorheen. Activiteiten in de fysieke dimensie blijven belangrijk, in de eerste plaats als afschrikking, maar ook om in te kunnen grijpen wanneer dat nodig is. Maar omdat onze slagkracht volledig scheef is opgebouwd in het licht van het moderne conflict is het noodzaak om nu expertise, operationele concepten en capaciteiten te ontwikkelen die de cognitieve en virtuele dimensies benutten, van strategisch tot tactisch niveau.

Gelukkig hebben we een groot menselijk kapitaal dat dit potentieel mogelijk maakt; hoogopgeleid, cultureel sensitief en met kritisch denkvermogen. Daarnaast hebben we een jongere generatie die in het informatietijdperk is opgegroeid en daardoor goed genetwerkt is, ook buiten de defensieorganisatie. Met de veranderende context van militair optreden en een hernieuwde analyse hoe we invulling moeten geven aan de bij wet aan ons toebedeelde taak,[9] worden de mensen in de organisatie niet ineens irrelevant. Mensen worden alleen maar irrelevant als ze niet in staat zijn om zich kwetsbaar op te stellen en kritisch te reflecteren op de context en zichzelf. Wie open staat voor verandering en vanuit een mindset van een leven lang leren een rol zoekt binnen de organisatie waar zij/hij tot haar/zijn recht komt, zal nooit overbodig zijn. We betogen niet dat mensen bewust de werkelijkheid anders voorspiegelen en de weergave van een modern conflict en de consequenties ervan voor de krijgsmacht expres verdraaien. Maar als we ons bewuster zijn van de subjectieve 'waarheden', associaties, aannames en vooroordelen en hoe deze onze perceptie, keuzes en handelen sturen, kunnen we de impact van gemotiveerd redeneren beperken. We moeten daarvoor dan eerst accepteren dat mensen geen neutrale informatieverwerkingssystemen zijn waarmee objectieve beeldvorming kan worden gerealiseerd. Ten slotte moeten we vorming gaan zien als het ontdekken en ontwikkelen van talent en niet als een middel om mensen voor het grootste deel in dezelfde mal te laten passen. Niet assimilatie en homogeniteit als streven, maar integratie en diversiteit in de organisatie, met behoud van dat wat iemand waardevol maakt.

Stilstand is achteruitgang: laten we dus in beweging komen. Want Defensie bestaat alleen maar omdat wij, mensen, er invulling aan geven. Wij kunnen en moeten dus zelf de verantwoordelijkheid nemen om veranderingen in gang te zetten. Dat is de enige manier om als krijgsmacht effectief op te kunnen treden tegen de dreiging van vandaag en de toekomst, niet die van het verleden. ■

8 Zie: Lawrence Freedman, *The Future of War. A History* (Londen, Penguin, 2017).

9 *Grondwet, Artikel 97*: Ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde, is er een krijgsmacht.

FOTO'S BEELDBANK NIMH

'Een lawine van geruchten en onware berichten'

'Ons volk is volkomen vertrouwd met gedrukten, films, luidsprekers, radio en straks de televisie. De inzet van deze middelen is zonder meer zeker.' Kapitein der infanterie J. Houtzagers schreef dat in 1956 in een artikel over de gevaren van de propagandamachine van de Sovjet-Unie voor Nederlandse militairen en burgers.[1]

Houtzagers waarschuwde voor 'fluistercampagnes, sabotage, agitatie en subversieve acties' en voor een 'lawine van geruchten en onware berichten.' Hij zag tevens het gevaar van de 'psychologische oorlog, gericht op onze burgerbevolking', met een directe negatieve invloed op het moreel van de strijdkrachten. Het uiteindelijke doel van deze manier van optreden in de Koude Oorlog was het ondermijnen van het vertrouwen in de leiding.

Het zwaartepunt bij de verdediging tegen beïnvloeding moest volgens Houtzagers bij de voorlichting liggen: 'zo de voorlichting goed wordt gevoerd immuniseert men de man tegen al de ideeën, tegen de gehele ideologie, die de tegenstander hem tracht op te dringen.' De kapitein pleitte er ook voor om eenheden tijdens oefeningen bewust bloot te stellen aan propaganda en dan tevens de uitwerking op het moreel te meten. Mocht het tot ernstinzet komen, dan was het mogelijk om vijandelijke propaganda tegen te gaan door het bezit van pamfletten te verbieden en radiouitzendingen te storen. Luidsprekers waarmee de tegenstander aan het front zijn boodschap verkondigde konden door artillerie en mortieren worden uitgeschakeld. Mislukte dat, dan was één van de oplossingen militairen op te dragen 'door het maken van lawaai (of zingen) de oproepen onverstaanbaar te maken.' ■

1 P.J. Houtzagers, 'Kan men zich verdedigen tegen psychologische oorlogvoering?', in: *Militaire Spectator* 125 (1956) (1) 20-29. Zie: https://www.militairespectator.nl/sites/default/files/bestanden/uitgaven/1918/1956/1956-0020-01-0010.PDF.

Het meten van militaire discipline of de wilde chaos

Jaus Müller MA[*]

Het is ongetwijfeld het hoogst haalbare in klassieke manoeuvre-oorlogvoering: zodanig verrassend manoeuvreren dat de vijand het overzicht verliest, in paniek raakt, vlucht en zich simpelweg overgeeft. Een schoolvoorbeeld is te vinden in mei 1940 in de laatste dagen van de Slag bij Sedan. Ten zuiden van Sedan, bij het plaatsje Bulson, lag in het bos de commandopost van generaal Lafontaine, commandant van de 55e infanteriedivisie. Die divisie had volgens plan met een tegenaanval de Duitse opmars in Frankrijk moeten afstoppen. Daar was tijd genoeg voor. Op 13 mei was de Duitse infanterie de Maas bij Sedan overgestoken. Op dat moment waren de Duitse tanks de rivier nog niet over. De Fransen dachten echter anders. De ongekende snelheid waarmee de Duitse militairen van de pantserdivisies dwars door de Ardennen trokken, leidde tot ongeloof bij de Fransen, die met achterhaalde tijd-ruimte-factoren rekenden. De Fransen bewezen dat angst een slechte raadgever is: op 13 mei, aan het begin van de avond, gaf een officier van een artillerie-eenheid in de buurt van Bulson melding van Duitse tanks (die hij onmogelijk kon hebben gezien). Hoewel het bericht niet klopte, voedde het de Franse vrees dat de Duitsers op talloze plekken opdoken. Paniek maakte zich daarom meester van zowel de 55e als delen van de 71e divisie. De mentale component van het militair vermogen was gebroken, de Fransen sloegen op de vlucht, soms wel tot 100 kilometer verderop. Een collectieve 'Panzerkampfwagen-angst' ontnam de Fransen de wil tot vechten, nog voor ze de tegenstander in de ogen hadden gekeken. De rest van de geschiedenis is bekend. Op 22 juni tekende Frankrijk de wapenstilstand.

Dit krijgshistorisch voorbeeld uit de meidagen van 1940 is nog altijd actueel. Het bevat een mengvorm van klassieke manoeuvre (de fysieke snelle opmars van de Duitse pantserdivisies door de Ardennen) en Information Manoeuvre avant-la-lettre (de snelle opmars leidde tot desinformatie en chaos aan Franse zijde). Het voorbeeld leest haast als een anachronistische uitwerking van wat nog steeds in onze eigen *Nederlandse Defensie Doctrine* staat: 'Een hoog operationeel tempo wordt bereikt door een snelle besluitvorming, door snelheid in de uitvoering en door snel te wisselen van activiteiten. Door dit hoge tempo kan de besluitvormingscyclus van de tegenstander worden verstoord, zodat hij niet meer adequaat kan reageren; zijn wil, samenhang en perceptie worden daardoor aangetast.'[1] Precies dát gebeurde bij de Fransen van de 55e divisie: de samenhang viel uiteen en de Duitsers ontnamen de Fransen de wil om te vechten. Maar geven we de Duitsers hier niet wat te veel schouderklopjes? Wisten zij werkelijk van tevoren dat hun fysieke manoeuvre zou worden gevolgd door een implosie van het Franse leiderschap in het informatie-domein? Wie de bronnen leest, komt tot de conclusie dat de Duitsers zelf net zo goed verrast waren door de Franse paniek bij Bulson.

Het voorbeeld laat ook zien hoe lastig het is om inzicht te krijgen in de mentale gesteldheid van de

* Op deze plaats vindt u afwisselend columns van Frans Matser en Jaus Müller.

1 *Nederlandse Defensie Doctrine* (Den Haag, ministerie van Defensie, 2019) 93.

tegenstander. Wanneer breekt die wil? Wat is het kantelpunt wanneer militaire discipline omslaat in wilde chaos? Er is geen tabel voor te vinden in het handboek stafgegevens. Als motivatie zich moeilijk laat meten, hoe kun je als militair dan plannen op het verwachte moment dat de vijand zijn wapens aan de wilgen hangt? Het grote probleem: niemand die het met zekerheid weet. In mei 1940 niet, en nu al helemaal niet. Onderzoek naar de mentale component is namelijk zoveel complexer dan het analyseren van slagkracht in het fysieke domein. De asymmetrische oorlogen na *9/11* hebben immers laten zien dat een militair oppermachtig land als de Verenigde Staten islamitische rebellenbewegingen, rondrijdend in hun ongepantserde Toyota Hilux, fysiek niet kan verslaan. De dreiging van militair spierballenvertoon en de paniek die dat teweeg kan brengen, zoals in Bulson in 1940, is een bot middel gebleken tegen islamitische terreurbewegingen. Hoe angstaanjagend ze ook mogen klinken, Hellfire-raketten of Daisy Cutters hebben de Taliban en IS de wil om te vechten bepaald niet ontnomen.

Het laat zien dat we anno 2020, midden in het informatietijdperk, op zoek moeten naar een middel dat wel werkt om de wil van de vijand te beïnvloeden. Onderzoek hiernaar staat pas in de kinderschoenen. Sterker nog: eigenlijk weten we helemaal niet eens waar we over praten, concludeerde het onderzoeksinstituut RAND in 2018 in het rapport *Will to Fight.* Het rapport signaleerde dat bij *information warfare* de kreet '*will to fight*' overal opduikt, zonder dat iemand precies kan vertellen wat daar eigenlijk in de moderne context mee wordt bedoeld: 'Our literature review of 202 published works, U.S. and allied military doctrine, 68 subject matter expert interviews, and several hundred additional sources on specific historical cases, war gaming, and simulation revealed no generally accepted military or scientific definition, explanation, or model of will to fight.'[2] De onderzoekers destilleerden uit de Amerikaanse doctrines en war games weliswaar drie componenten (moreel, cohesie en discipline) voor het bepalen van de will to fight, maar ook die termen verzanden vaak in vaagheid.

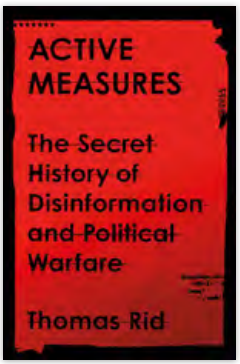
Militair overwicht alleen is niet genoeg meer: anno 2020, midden in het informatietijdperk, moeten we op zoek naar middelen die wel werken om de wil van de vijand te beïnvloeden

Loskomen van de algemeenheden uit de doctrines vereist meer duiding en onderzoek om tot een beter begrip van gevechtsbereidheid te komen. De VS schakelde hiervoor de denktank Artis International in. Om beter te begrijpen wat zich op de grond in Irak afspeelt, gingen vijfenveertig veldonderzoekers op pad. Zij vroegen Iraakse soldaten, Peshmerga-strijders, Soenni-militieleden en gevangengenomen IS-strijders naar hun bereidheid om de strijd voort te zetten. Hun antwoorden categoriseerden de onderzoekers op een gevechtsbereidheids-schaal met 7 punten. Een van hun lezenswaardige conclusies, waarover weekblad *The Economist* begin september bericht-te, was dat de wil om te vechten het sterkst was bij hen die de minste waarde hechtten aan materiële welvaart en economische vooruitzichten.[3] Het veldwerk liet bovendien zien hoeveel slachtoffers een moderne (irreguliere) eenheid kan verdragen voordat zij er als collectief mee ophoudt, en hoe de factoren informatievoorziening en angst daarop inwerken.

Het lijkt me nuttig onderzoek, waarmee we in de toekomst een nieuwe 'paniek van Bulson' mogelijk kunnen voorkomen, of juist kunnen creëren, maar dan bij de vijand. Maar erger dan de chaos bij de 55e infanteriedivisie kan het volgens mij nooit worden. Divisiecommandant Lafontaine liet in de chaos in de meidagen per abuis zijn eigen commandopost in brand steken. Verstoken van alle verbindingen reed de generaal vervolgens uren in zijn stafauto van niets naar nergens om persoonlijk totaal achterhaalde orders af te geven, terwijl de Duitsers hun opmars vervolgden. ■

2 Ben Connable e.a., *Will to Fight. Analyzing, Modeling, and Simulating the Will to Fight of Military Units* (Santa Monica, Rand Corporation, 2018) xii.

3 'What motivates the dogs of war', in: *The Economist* (5-11 september 2020) 63-65.



Active Measures

The Secret History of Disinformation and Political Warfare
Door Thomas Rid
New York (Farrar, Straus and Giroux) 2020
528 blz.
ISBN 9780374718657
€ 26,-

Na de presidentsverkiezingen in de Verenigde Staten van 2016 zijn er meerdere onderzoeken geweest naar buitenlandse beïnvloeding, primair vanuit Rusland. Op 30 maart 2017 verschijnt ook Thomas Rid als deskundige voor de Select Committee on Intelligence van de Amerikaanse Senaat om te spreken over desinformatie en Russische beïnvloedingsoperaties, niet zozeer om bewijs te leveren, maar om een analyse te geven van de concepten van Russische beïnvloeding.[1] De poging om de Amerikaanse verkiezingen te beïnvloeden was geen incident. Rusland, en voorheen de Sovjet-Unie, is met beïnvloedingsoperaties en *active measures* al decennia bezig om de fundamenten van de liberale democratische orde te ondermijnen. En hoewel Rid zich richt op de activiteiten van Rusland, voormalig Oost-Duitsland en Tsjechoslowakije, geeft hij aan dat ook de VS, met name de CIA, soortgelijke operaties uitvoert.

Desinformatiecampagnes

Active measures zijn activiteiten om desinformatiecampagnes uit te voeren. Rid geeft in zijn boek geen duidelijke omschrijving van active measures of van het verschil tussen active measures en desinformatie, maar hij geeft wel aan dat active measures weloverwogen acties zijn en de inhoud van die activiteit bevat altijd een element van desinformatie. Denk daarbij aan het vervalsen van informatie, of informatie op een bepaalde manier presenteren door te veel data te geven of elementen weg te laten of anders te verwoorden. De active measures zijn wellicht terug te voeren tot een pamflet van Lenin uit 1902 over hoe massa's te mobiliseren zijn, waarbij de active measures – met een knipoog naar Von Clausewitz' 'oorlog als voortzetting van politiek met andere middelen' – een voortzetting van oorlog met andere middelen zouden zijn. Een active measure is daarmee een instrument om een specifiek (politiek) doel te bereiken, en zeker geen 'leugentje om bestwil'.

Om de hedendaagse Russische beïnvloedingsoperaties te begrijpen en er tegen te ageren is er volgens Rid maar één vaccin: teruggrijpen naar het verleden en analyseren hoe technologische en culturele ontwikkelingen de active measures hebben gevormd.

Rid beschrijft de ontwikkeling van active measures en desinformatie door de jaren heen. In de eerste periode van het Interbellum tot aan het einde van de Tweede Wereldoorlog kenmerken de activiteiten zich door klassieke misleiding, vervalsingen van documenten en soms door journalisten – gebrand op een *scoop* – voor het karretje te spannen. Desinformatie is in deze fase nog het wapen van de armen en de zwakken, die daarmee grote en machtige vijanden op asymmetrische wijze kunnen aanvallen. Na de Tweede Wereldoorlog professionaliseerde desinformatie, niet in de laatste plaats omdat twee grote machtsblokken, Amerika en Rusland, nu tegenover elkaar kwamen te staan met ieder een eigen ideologie. In Amerika, met de CIA voorop, ontwikkelde zich het fenomeen van *political warfare*, waarbij de opponenten worden beïnvloed met een combinatie van onthullingen van oprechte waarheden, misleidingen door vervalsingen, of het subversief ondermijnen van de perceptie. Rusland en zijn satellietstaten hadden het over 'desinformatie'. Maar ondanks de andere naam was het doel in beide gevallen het versterken van bestaande spanningen en tegenstellingen in het politieke bestel van de opponent, gebruikmakend van waarheden en onwaarheden, of beter nog, een desoriënterende mix van beide.

Vanaf midden jaren 70 van de vorige eeuw tot de val van de Berlijnse Muur in 1989 begint Rusland dominant te worden, niet in de laatste plaats omdat Amerika ervan uit gaat dat de actieve beïnvloeding na de bouw van de Berlijnse Muur plaatsmaakt voor andersoortige wedkampen – de nucleaire afschrikking. Hoewel de desinformatie in

1 Thomas Rid, 'Disinformation: A Primer in Russian Active Measures and Influence Campaigns' (Washington, D.C., Select Committee on Intelligence United States Senate, 2017).

beide machtsblokken wordt ingebed in bureaucratische structuren en onderdeel gaat uitmaken van een van de instrumenten van macht, is de Russische beïnvloeding veel actiever. Rid beschrijft gedetailleerd hoe Rusland de vredesbeweging in het Westen heeft aangewakkerd om te voorkomen dat er Amerikaanse kernwapens in West-Europa worden geplaatst en licht ook toe hoe de ontdekking van aids wordt gebruikt om bestaande maatschappelijke tegenstellingen en sentimenten (tegen homoseksuelen, drugsverslaafden en immigranten) te verscherpen. De Russische active measures draaien op volle toeren, tot de val van de Berlijnse Muur.

In de jaren 90 lijkt Rusland richting een democratische samenleving te transformeren, waarbij de desinformatiecampagnes aan beide zijden op een laag pitje staan. Maar niet lang. Met de opkomst van Vladimir Poetin wordt desinformatie langzaam herontdekt, gerevitaliseerd en zelfs geïnnoveerd als gevolg van nieuwe digitale technologie, met name internet en later de sociale media. Het inbreken op computersystemen (hack) en vervolgens verspreiden van informatie die eigenlijk geheim had moeten blijven (leak) wordt tot kunst verheven. Het internet lijkt bij uitstek geschikt voor active measures en desinformatiecampagnes. Maar cyberspace en het internet maken het ook mogelijk dat iedereen zich mengt in de arena van desinformatie, van het Yemen Cyber Army dat Saudi-Arabië hackt tot aan actieve socialemediagebruikers die onbedoeld active measures versterken. De active measures zijn daardoor veel minder te controleren en te sturen. Ze worden daardoor *more active* en *less measures*.

Duivels dilemma

Rid destilleert een aantal conclusies uit zijn historische overzicht. Ten eerste: na de bouw van de Berlijnse Muur in 1961 zijn de Amerikaanse activiteiten op het terrein van desinformatie afgenomen, terwijl de Sovjet-Russische zich juist verder bleven ontwikkelen. Daardoor is een parallax tussen beide ontstaan, temeer doordat in de jaren 70, onder invloed van het postmodernisme, de objectieve waarheid deels onderuit is gehaald door te stellen dat de waarheid een construct is, gebaseerd op een ideologie en niet op een analyse. Een ontwikkeling waarvan de Russische active measures gebruik lijken te maken, maar de Amerikaanse minder. Dit komt tevens doordat westerse democratieën kennis en daarmee 'de waarheid' boven gevoelens stellen, bewijs boven emotie en observaties boven opinies. Active measures zijn effectief, niet wanneer zij 'waar' zijn, maar wanneer ze de gevoelens van de bevolking weergeven. Dat desinformatiecampagnes het hart van onze democratieën raken is dan ook Rids tweede conclusie. Desinformatieoperaties ondergraven de autoriteit van bewijsvoering, een gat dat wordt opgevuld door emoties en opinies, met als gevolg dat de waarheid bijna niet meer van de leugen te onderscheiden is. Gevolg is wel dat een desinformatiecampagne tevens zichzelf kan ondergraven. En de digitale revolutie, tot slot, heeft desinformatie fundamenteel veranderd.

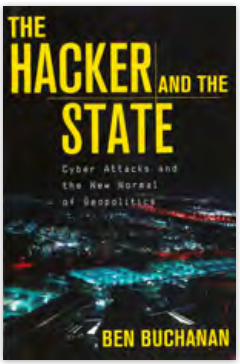
Active Measures van Thomas Rid is een *must-read* voor iedereen die geïnteresseerd is in hedendaagse beïnvloedingsoperaties en desinformatie, ongeacht vanuit welk land. Rid geeft veel inzicht hoe beïnvloedingsoperaties werken en hoe de kwetsbaarheden in een samenleving of bij groepen in die samenleving kunnen worden uitgebuit. Hij presenteert zijn kennis met vele cases, die hij soms als een anekdote vertelt, waardoor het boek goed leesbaar is. De vraag is echter wel of Rids vaccin gaat werken: hij interpreteert de active measures als een poging om liberale democratieën te ondermijnen. Maar acties om dat tegen te gaan druisen ook in tegen de fundamenten van het democratische systeem. Een duivels dilemma! ■

Kol mr. drs. B.M.J. Pijpers, FMW/NLDA

Schrijft u een gastcolumn in de *Militaire Spectator*?

De redactie van de *Militaire Spectator* biedt lezers de mogelijkheid een gastcolumn te schrijven van maximaal duizend woorden. Het thema is vrij, maar moet passen in de formule van het tijdschrift. Een gastcolumn bevat een relevante boodschap voor de lezers, een gefundeerde eigen mening en juiste en verifieerbare feiten in een logisch opgebouwd betoog. 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



The Hacker and the State

Cyber Attacks and the New Normal of Geopolitics
Door Ben Buchanan
Cambridge (Harvard University Press) 2020
412 blz.
9780674987555
€ 24,-

Voor diegenen die geïnteresseerd zijn in de combinatie van cyber en geopolitiek is het nieuwste boek van Ben Buchanan een aanrader. In *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics* beschrijft hij op een redelijk technische, maar zeer toegankelijke wijze, hoe cyberaanvallen geopolitieke ontwikkelingen beïnvloeden en vormgeven. Ben Buchanan komt uit de school van Thomas Rid en schreef zijn proefschrift bij hem op King's College in Londen. Rid is een van de eerste onderzoekers die het debat over cyberoorlog voorzag van structuur en conceptuele helderheid met zijn boek *Cyber War Will Not Take Place* (2013).
Buchanan loopt zijn onderzoek naar cyberoperaties aan vanuit de academische discipline internationale betrekkingen, en in zijn eerste boek *The Cybersecurity Dilemma* (2017) legde hij overtuigend uit hoe het veiligheidsdilemma (*security dilemma*) verscherpt wordt door de unieke kenmerken van het cyberoptreden. Doordat offensieve en defensieve cyber dicht bij elkaar liggen en voor vijandelijke staten vaak moeilijk van elkaar te onderscheiden zijn, neemt het onderlinge wantrouwen alleen maar verder toe. Buchanans boek *The Hacker and the State* heeft een bredere opzet: het geeft een gedetailleerd overzicht van alle grote (bekende) cyberoperaties tot nu toe en plaatst de casuïstiek in de context van algemeen geopolitiek optreden.

The new normal

The Hacker and the State bevat voor niet-ingewijden waardevolle analyses die vervlochten zijn in het geheel. Een eerste constatering is dat cyber niet goed vergeleken kan worden met kernwapens. Veel analisten en onderzoekers hebben in het verleden cyber juist vanuit het nucleaire paradigma benaderd, als een digitaal equivalent van kernwapens: enorm vernietigend, maar zeldzaam. Buchanan toont aan dat dit onterecht is. Cyberaanvallen zijn inmiddels niet zeldzaam meer, maar juist *the new normal*. Er gaat immers geen week voorbij zonder nieuws van een grote hack, een datalek of ontdekte gevallen van cyberspionage of cybersabotage. Cyberaanvallen, schrijft hij, 'have become a low grade yet persistant part of geopolitical competition' (blz. 3). Juridisch en sociologisch gezien is wellicht de term oorlog hier niet passend, maar staten blijken aanhoudend met elkaar in een digitale strijd te zijn verwikkeld. Deze strijd speelt zich af buiten het zicht van het publiek en wordt vaak niet goed begrepen door traditionele veiligheidsexperts (en politici).
Een tweede rode draad is dat natiestaten geen monopolie hebben op operaties en activiteiten in cyberspace. Bedrijven en criminele organisaties zijn minstens even belangrijke actoren in de zogeheten mêlee, en dit compliceert het toepassen van traditionele theorieën uit de discipline van internationale betrekkingen.

Het conceptuele kader van het boek is eenvoudig. Landen voeren geopolitiek door middel van *signaling* en *shaping*. Onderzoek in internationale betrekkingen richt zich nog voornamelijk op het eerste en dit omvat hoe staten signalen afgeven om hun standpunten en hun intenties duidelijk te maken. Nucleaire wapens geven bijvoorbeeld een afschrikwekkend signaal af en het mobiliseren of ontplooien van militaire eenheden kan eveneens een duidelijke boodschap geven aan potentiële tegenstanders. Shaping daarentegen betreft het direct beïnvloeden of smeden van het gedrag van de ander, door deze bijvoorbeeld te destabiliseren door bedrog, sabotage of andere heimelijke activiteiten. Buchanan past dit conceptueel kader vervolgens toe op een reeks casussen van cyberoperaties. De essentie van zijn argument is dat het cyberinstrumentarium niet geschikt is voor signaling, maar wel erg effectief is op het gebied van shaping. Dit wordt nader uitgewerkt in de drie delen van het boek – spionage, aanval en destabilisatie. Deze delen omvatten elk meerdere hoofdstukken, alle gecentreerd rond een aantal bekende incidenten of cyberoperaties die in detail worden weergegeven.

Beschrijving grootste cyberaanvallen
Het boek is alleen al waardevol omdat het een overzichtelijke beschrijving biedt van de grootste cyberaanvallen van de afgelopen tien jaar. Veel van deze zijn al uitvoerig elders beschreven, zoals de beroemde Amerikaans-Israëlische Stuxnet-cyberaanval op de uraniumverrijkingsinstallatie in Natanz, Iran. Buchanan vat de bekende verhalen beknopt samen en voegt de meest recente informatie toe, zoals de *scoop* van *Volkskrant*-journalist Huib Modderkolk bij Stuxnet. Modderkolk meldde dat het een agent van de AIVD was die het virus door middel van een USB-stick overbracht naar het Iraanse netwerk en daarmee de *air gap* overbrugde (waarmee het lokale netwerk van het internet gescheiden was). Andere bekende voorvallen zijn de reeks van Chinese operaties om intellectueel eigendom te stelen (bedrijfsspionage), de Sony-hack, de Noord-Koreaanse digitale beroving van verschillende banken, de Wannacry- en NotPetya-aanvallen, Sandworm en de Oekraïense energiecentrales: allemaal passeren ze uitgebreid de revue. Ook wijdt Buchanan een hoofdstuk aan de Russische inmenging in de Amerikaanse presidentsverkiezingen van 2016. Dit omvatte zowel een *hack & leak*-element waarbij e-mails van de Democratic National Committee werden gelekt, als een uitgebreide campagne waarbij desinformatie werd verspreid.

Shadow Brokers
Voor het eerst in de cybersecurity-literatuur heeft Buchanan de casus van de Shadow Brokers uitgewerkt en opgeschreven. Tussen najaar 2016 en lente 2017 bracht een onbekende groep die zichzelf de Shadow Brokers noemde een aantal *exploits* van de Amerikaanse National Security Agency (NSA) naar buiten. Dit betrof verschillende zeer geavanceerde *hacking tools* die kwetsbaarheden in onder meer Windows uitbuitten. De bekendste van deze heette ETERNAL BLUE. Nadat de Shadow Brokers dit 'cyberwapen' op internet zetten, werd het door Noord-Koreaanse en Russische hackers geïntegreerd in hun eigen cyberaanvallen (in respectievelijk Wannacry en NotPetya). Het NSA-'wapen' was zo krachtig dat Microsoft-president Brad Smith het vergeleek met de diefstal van een paar Tomahawk-kruisraketten uit het Amerikaanse arsenaal. Zo heeft de NSA ongewild een belangrijke bijdrage geleverd aan de NotPetya-aanval die uiteindelijk wereldwijd meer dan 10 miljard dollar aan schade aanrichtte. Het is nog steeds niet duidelijk wie achter de Shadow Brokers zat, maar Buchanan vermoedt – waarschijnlijk terecht – dat de Russische inlichtingendiensten een rol hebben gespeeld. Dit lek was uiteindelijk vele malen schadelijker dan dat van Edward Snowden enkele jaren eerder.

Naming and shaming
Zoals elk boek kent *The Hacker and the State* ook enkele onvolkomenheden. Het theoretisch kader is minder robuust dan in Buchanans eerdere boek. Zo passen bijvoorbeeld spionage en inlichtingenvergaring, waar het gros van statelijke cyberoperaties onder valt, niet altijd goed in de categorie shaping. Sommige hoofdstukken beschrijven weliswaar goed de gekozen cyberoperaties, maar geven slechts een summiere analyse hoe ze zich verhouden tot de theorie. Ook blijkt het lastig te categoriseren tussen inlichtingendiensten die criminele activiteiten ontplooien om geld te verdienen voor hun regime (Noord-Korea); zij die vervlochten zijn met de georganiseerde misdaad (Rusland); of zij die hackers in dienst hebben die er naast hun dagtaak een eigen cyber-zzp'tje op nahouden (Rusland en China). Inhoudelijk worden sommige van Buchanans conclusies ook niet gesteund door de feiten. Zo meent hij bijvoorbeeld dat het veelvoud aan FBI-*indictments* (dagvaardingen) maar weinig geopolitiek effect heeft gehad (blz. 99 en 305). Maar er is wel degelijk bewijs dat *naming and shaming* werkt. Op operationeel vlak hebben statelijke hackers vaak hun digitale aanvalsinfrastructuur moeten opgeven nadat deze door de FBI of IT-bedrijven werd ontmaskerd. Nieuwe tactieken en technieken moesten dus worden ontworpen omdat de oude verbrand waren. Ook op het diplomatieke vlak hebben China en Rusland aanzienlijke reputatieschade geleden. Vooral China was woest dat de VS in 2014 grote WANTED-posters verspreidde met Chinese militairen afgebeeld in uniform. Dit heeft, samen met het dreigement om sancties toe te passen, in 2015 geleid tot een akkoord tussen China en de VS om geen cyberbedrijfsspionage meer uit te voeren. Het akkoord heeft overigens niet lang standgehouden; inmiddels is het weer schering en inslag op dit gebied.

Ondanks deze kleine punten is *The Hacker and the State* een zeer lezenswaardig boek dat een plek verdient in de boekenkast. Als ouderwetse hardcopy natuurlijk, want alles wat digitaal is betekent kennelijk een risico. ■

Sergei Boeke, politiek adviseur NAVO-hoofdkwartier Joint Support & Enabling Command (JSEC) Ulm

Een flintertje moed

Linda Polman

Turkije vindt dat de gasvoorraad onder de oostelijke Middellandse Zee-bodem 'grijs gebied' is: Griekenland zégt er het alleenrecht op te hebben, maar volgens Turkije interpreteren de Grieken de internationale rechten verkeerd. Turkije stuurde seismische schepen, begeleid door oorlogsbodems en F-16-straaljagers, op de gasvelden af om ze leeg te boren. In antwoord kondigden de Grieken de aanschaf aan van achttien nieuwe gevechtsvliegtuigen, fregatten, helikopters, torpedo's, raketten en antitankgeschut en beloofde 15.000 nieuwe rekruten te gaan werven. 'Één vonkje erbij in dat kruitvat en we kijken naar een catastrofe', zei een bezorgde Duitse minister van Buitenlandse Zaken.

Het is altijd hommeles tussen Turkije en Griekenland. Om wat dan ook. In 2006 waren de Turken woedend toen de EU voor toeristen affiches maakte met reclame voor Griekenland als uitvinder van de mierzoete baklava. In 2012 werd in die strijd een nieuw front geopend toen president Obama in het Witte Huis baklava op tafel liet zetten door een Griekse kok tijdens een diner ter ere van de Griekse Dag van de Onafhankelijkheid. Turkije liet de wereld onmiddellijk weten dat Obama's hele diner, van de baklava tot de moussaka en gevulde druivenbladeren aan toe, allemaal Turkse gerechten waren en dat de Grieken altijd met Turkse veren proberen te pronken.

Vooral gaat de Turks-Griekse vete over de status van Cyprus. In 1974 viel Turkije Cyprus binnen en bezette het noordelijke deel. Een wandeling door dat conflict begon in een nauwe straat in hoofdstad Nicosia, bij het wrak van een gele auto. Banden en ramen ontbraken. De auto stond daar decennia lang precies op de Groene Lijn, waar VN-blauwhelmen sinds 1974 de Turken en de Grieken uit elkaar houden. De Grieks-Cyprioten hielden vol dat de grens vanaf het linkerachterwiel van de gele auto naar een muur liep. De Turken zeiden dat die vanaf het linkervoorwiel liep. De wandeling eindigt nog steeds in de kelder van een garagebedrijf, waar tientallen Japanse auto's staan die net voor de Turkse invasie door een Griekse autohandelaar waren geïmporteerd. De Toyota's staan er nog steeds, omdat de enige uitgang van de showroom aan de Turkse kant van de stad uitkomt.

Turkije heeft er zin in. In 2019 viel het Syrië binnen, intervenieerde in Libië, kocht Russisch militair materieel en nu dreigt het Europa met oorlog om het Griekse gas. Als voorzitter van Europa moet Duitsland het vuur zien te doven, maar het kan partijen slechts vriendelijk verzoeken om met elkaar in dialoog te treden: voor méér dan dat gaven de EU-lidstaten Duitsland geen mandaat. Niets wijst erop dat Europese leiders van plan zijn om de strijd met Turkije aan te gaan, want zij weten dat zij aan hun achterban het verlies van een beetje Grieks gas duizendmaal makkelijker zullen kunnen verkopen dan de komst van nieuwe vluchtelingen. Want zo speelt Turkije het: steeds als het van Europese leiders iets gedaan wil krijgen zet het zijn poorten op een kier en zien wij tot onze afschuw er weer wat binnenkomen. Het Nederlandse kreunen en tandenknarsen vooraf aan het besluit om honderd vluchtelingen uit Moria toe te laten, bewees weer dat Turkije door Europa nooit verslagen zal kunnen worden: de vier miljoen vluchtelingen op Turks grondgebied ontnemen Europese leiders elk flintertje moed. ■

The Cyber Defense Review

Special Edition: Information Operations/ Information Warfare
Vol. 5, No. 2, Summer 2020
Door Andrew O. Hall en Robert J. Ross (red.)
West Point (Army Cyber Institute) 2020
148 blz.
Te downloaden via: https://cyberdefensereview.army.mil

Information Operations en Information Warfare zijn niet nieuw, maar de 'exponential adoption and weaponization of social media technologies' veranderen het karakter van het hedendaagse conflict. Vanuit dat uitgangspunt belichten experts van de Amerikaanse strijdkrachten in een special van *The Cyber Defense Review* de uitdagingen om een 'information advantage' te verkrijgen en te behouden ten opzichte van tegenstanders die chaos en polarisatie willen veroorzaken. De auteurs wijzen onder meer op juridische en morele vraagstukken bij het counteren van desinformatie en de urgentie van de verdediging tegen *storyweapons*, gedefinieerd als 'adversarial narratives that use algorithms, automation, codespaces, and data to hijack decision-making'.

How to Lose the Information War

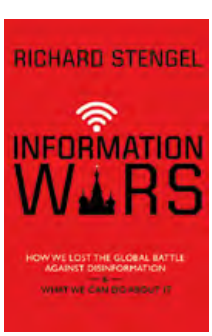
Russia, Fake News, and the Future of Conflict
Door Nina Jankowicz
Londen (IB Tauris) 2020
288 blz.
ISBN 9781838607685
€ 30,-

In *How to Lose the Information War* kijkt Nina Jankowicz naar Russische desinformatiecampagnes in de VS, Estland, Georgië, Polen, Tsjechië en Nederland. Volgens Jankowicz is het Westen terecht gealarmeerd door de Russische inmenging in de Amerikaanse presidentsverkiezingen in 2016, hetzelfde jaar waarin de Russen een desinformatiecampagne voerden rond het Oekraïnereferendum in Nederland. Jankowicz noemt dat laatste een duidelijke aanval op de Europese democratie. Zij kwalificeert alle Russische initiatieven op informatiegebied als 'beïnvloedingsoperaties'. Een gezamenlijke westerse aanpak is lastig, omdat het Kremlin doelbewust campagnes voert die zijn toegesneden op de specifieke interne problemen van democratische landen.

Disinformation's Societal Impact: Britain, Covid, and Beyond

Door Thomas Colley e.a.
Defence Strategic Communications, Vol. 8, Spring 2020
Riga (NATO Strategic Communications Centre of Excellence) 2020
Te downloaden via: https://www.stratcomcoe.org

In hun artikel 'Disinformation's Societal Impact: Britain, Covid, and Beyond' in het tijdschrift *Defence Strategic Communications* gaan Thomas Colley, Francesca Granelli en Jente Althuis in op de gevolgen van desinformatie voor de cohesie en het vertrouwen in een samenleving. Volgens de auteurs is het onderzoek daarnaar niet coherent, en gaat de meeste aandacht van wetenschappers uit naar de manieren waarop desinformatie zich verspreidt. Beleid voor het tegengaan van desinformatie zou dan ook te veel gericht zijn op de vermoedelijke impact en niet op de werkelijke. In deze aflevering van *Defence Strategic Communications* is ook een artikel opgenomen over de stand van het debat rond *fake news*.



Information Wars

How we lost the global battle against disinformation and what we can do about it
Door Richard Stengel
New York (Grove Atlantic) 2019
368 blz.
ISBN 9780802147981
€ 25,-

Desinformatie is al zo oud als de mensheid. Door de opkomst van sociale media heeft het begrip echter een vlucht genomen. In toenemende mate gebruiken overheden en andere actoren desinformatie als wapen, waarop democratische systemen maar moeilijk een antwoord kunnen vinden. De auteur van *Information Wars* maakte als medewerker van de regering-Obama deze strijd van dichtbij mee. Richard Stengel put uit zijn ervaring als hoge ambtenaar op het Amerikaanse State Department, waarbij hij te maken kreeg met desinformatie door IS, het Rusland van Poetin, en later presidentskandidaat Donald Trump. Hij betoogt dat deze zeer diverse actoren in feite hetzelfde draaiboek gebruikten om hun boodschap te verkondigen.


Instagram
Phoster