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-

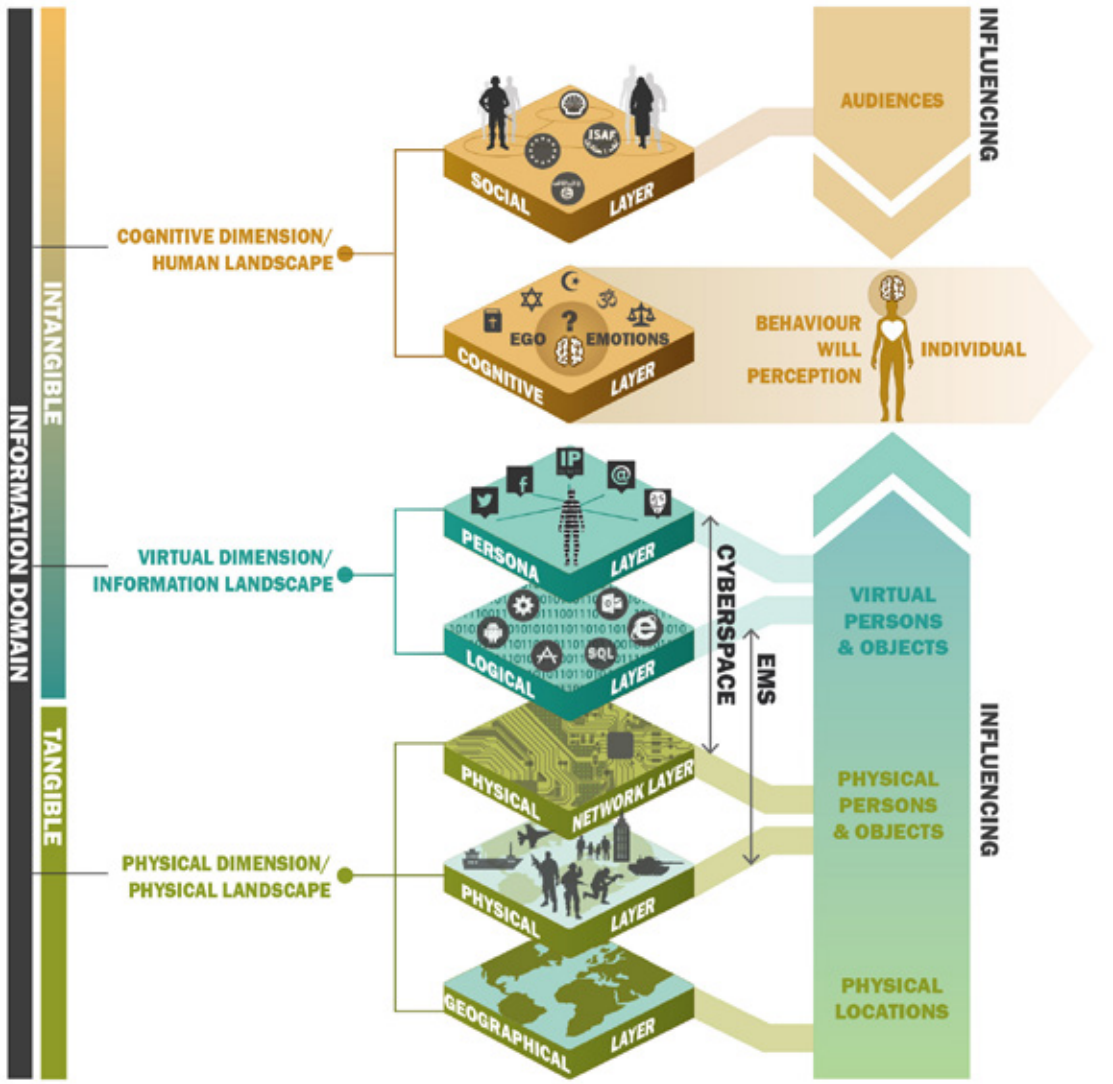
17 Bill Gertz, *iWar,* 'How the US can beat China, Russia, Iran, North Korea and Islamic Terrorists on the Digital Battlefield', 7.

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. ■