Waar is de onzichtbare vijand?

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

Op 24 november 2011 vierde de Koninklijke Militaire Academie van de Nederlandse Defensie Academie haar 183ste Dies Natalis. De Diesrede werd uitgesproken door prof. dr. B.G.J. de Graaff, hoogleraar inlichtingen- en veiligheidsstudies aan de NLDA en de Universiteit Utrecht. De redactie acht zijn thema dermate relevant en actueel dat zij, met instemming van de spreker, besloot de (geannoteerde) tekst in de Militaire Spectator te publiceren.

De hoofdredacteur

Excellenties, vlag- en opperofficieren, hoogleraren, dames en heren en natuurlijk cadetten en adelborsten. U bent in groten getale gekomen om te luisteren naar een rede met een mysterieuze titel. Aan het slot van mijn toespraak zult u hopelijk enigszins begrijpen welke bedoelingen ik had met deze lezing over de dreigingsomgeving van het Westen in het algemeen en de Nederlandse krijgsmacht in het bijzonder, alsmede mogelijke reacties daarop.

Ik ben langer dan alleen vandaag op de NLDA en in uw midden; dus het zal mogelijk zijn om in de komende tijd de gedachtewisseling omtrent dit onderwerp voort te zetten. Vandaag zult u, wellicht met een gevoel van machteloosheid, zijn onderworpen aan het door mij gesproken woord, maar ik bied u in de toekomst graag de gelegenheid tot repliek.

Inleiding

'They're coming after us. But who are they now?'

De essentie van het militaire bedrijf is de uitschakeling van vijanden, het liefst zonder toepassing van geweld, maar desnoods mét. Dat is voor mensen trouwens nog niet zo eenvoudig. In zogeheten linieoorlogen, waarin soldaten lijnrecht tegenover elkaar stonden, moest soldaten geleerd worden daadwerkelijk op elkaar te schieten. Ook in de Amerikaanse Burgeroorlog gebruikten nog veel soldaten hun geweer aanvankelijk in het geheel niet; anderen schoten bewust over de hoofden van de tegenstanders. Tijdens de Tweede Wereldoorlog bleek nog geen twintig procent van de militairen op hun tegenstander te hebben geschoten wanneer zij die in het directe zicht hadden. Pas vanaf 1945 kwam de *drill to kill* echt op gang. En met succes: in de Korea-oorlog bleek 55 procent van de soldaten bereid hun directe tegenstander te doden en in de Vietnam-oorlog was het cijfer zelfs gestegen tot 95 procent.[1]

In de loop van de geschiedenis is de technische mogelijkheid gegroeid om vijanden op steeds grotere afstand te lijf te gaan. Tegenwoordig besturen 'piloten' *drones* boven Afrika en Azië vanuit een woestijn in de Verenigde Staten en inmiddels lijkt er steeds meer een drill nodig te zijn om *niet* te doden, aangezien zich bij gevechtshandelingen op zulk een afstand ongewenste verschijnselen van *moral*

1 B. de Graaff, 'Leed meten', Chr. van der Heijden (red.), *Voorbij maar niet verdwenen. 65 jaar na de Tweede Wereldoorlog*, Den Haag 2010, p. 16.

disengagement, dehumanisering en de-individualisering voordoen.[2]

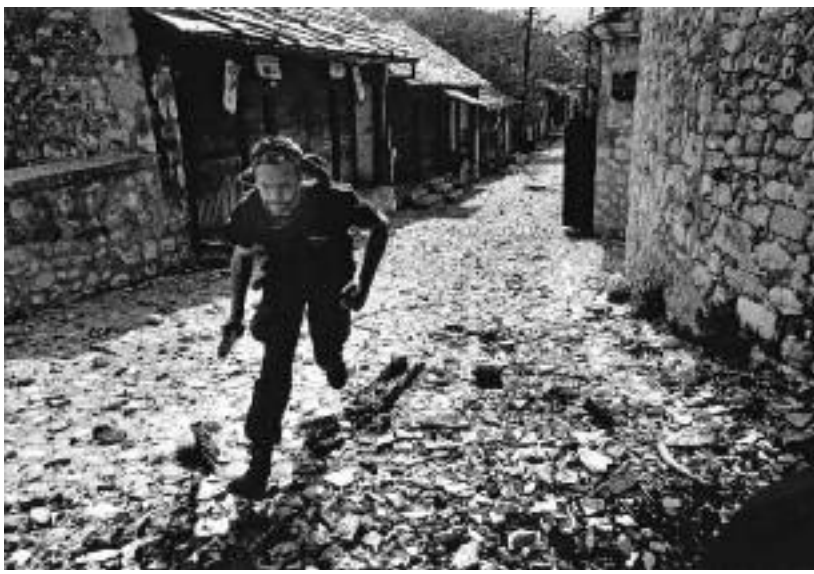
In hedendaagse conflicten is de vijand beslist niet altijd onzichtbaar. Nederlandse militairen, die bijvoorbeeld hebben geopereerd in de oorlog in Bosnië of nog recenter in het Afghaanse Uruzgan, kunnen daarvan meepraten.

Toch lijkt op veel fronten de vijand in tal van opzichten onzichtbaar geworden. Sterker nog, er bestaat veel onzekerheid over de vraag wie de vijand en wat de dreiging is, of enigszins eufemistisch uitgedrukt: er is sprake van 'hybride dreigingen' en *'blurred challenges'*.[3] Er wordt wel veel gespeculeerd over de aard van een toekomstig conflict, maar men komt over het algemeen weinig tegen over de vermoedelijke tegenstander.[4] Door het grote aantal potentiële vijanden dreigt het *intelligence* apparaat van zelfs de grootmacht Amerika overbelast te raken.[5] Wat leidt tot de vraag: '*They're coming after us. But who are they now?*'[6] Over dat uitgangspunt en de conclusies die daar al dan niet aan verbonden (moeten) worden, wil ik het vanmiddag hebben.

Onzichtbaarheid als dreiging

Generaal William T. Sherman, die wel is gekarakteriseerd als 'de eerste moderne generaal',[7] noemde generaal Ulysses S. Grant, onder wie hij in de Amerikaanse burgeroorlog diende, een uitstekende commandant. De reden die Sherman voor dit compliment gaf, was dat Grant zich volgens hem nooit had beziggehouden met de vraag wat de vijand aan het doen was wanneer die niet in zicht was.[8] Deze uit-het-oog-uit-het-hoofd-benadering van Grant en Sherman lijkt op het eerste gezicht beslist niet modern te noemen. Reeds tijdens de Amerikaanse burgeroorlog kwam de eerste moderne onderzeeër in actie, een halve eeuw later hadden vliegtuigen hun oorlogsdoop, om slechts twee wapens te noemen waarvan strijdende partijen graag wisten wat die aan het doen waren wanneer zij uit het zicht waren. Want, zoals het duo Van Kooten en De Bie al eens in een humoristische sketch vaststelde: de gevaarlijkste onderzeeërs zijn die welke je niet ziet.[9]

FOTO HOLLANDSE HOOGTE, T. VOETEN



In hedendaagse conflicten, waaronder Bosnië, is de vijand beslist niet altijd onzichtbaar

Anders gezegd: onzichtbaarheid is op zich al een dreiging. Een onzichtbare dreiging is dus een dubbele dreiging. Zij kan leiden tot strategische verrassing. Of, zoals de hoogste Amerikaanse inlichtingenautoriteit, de *Director of National Intelligence*, Dennis Blair, het in 2010 in de jaarlijkse dreigingsanalyse van de Amerikaanse inlichtingendiensten verwoordde:

2 Zie bijvoorbeeld N. Sharkey, 'Saying "No!" to Lethal Autonomous Targeting', *Journal of Military Ethics*, vol. 9 (2010) no. 4, p. 381; M.E. O'Connell, 'Seductive Drones: Learning from a Decade of Lethal Operations', *Journal of Law, Information & Science*, augustus 2011.

3 Zie bijvoorbeeld N. Freier, 'The Defense Identity Crisis: 'It's a Hybrid World', *Parameters*, augustus 2009; D. Sadowski & J. Becker, 'Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare', *smallwarsjournal.com*, 7 januari 2010. Vgl. K. Naumann e.a., *Towards a Grand Strategy for an Uncertain World. Renewing Transatlantic Partnership*, 2008; D. Thomas, 'U.S. Military Intelligence Analysis: Old and New Challenges', R.Z. George and J.B. Bruce (eds.), *Analyzing Intelligence. Origins, Obstacles, and Innovations*, Washington D.C. 2008, 146.

4 Zie bijvoorbeeld The Hague Centre for Strategic Studies, *Contours of Conflict in the 21st Century. A Cross-Language Analysis of Arabic, Chinese, English and Russian Perspectives on the Future Nature of Conflict*, The Hague 2011.

5 Thomas, 'Intelligence', 148-149; M.M. Lowenthal, 'Intelligence in Transition: Analysis after September 11 and Iraq', George & Bruce (eds.), *Intelligence*, 230.

6 D. Frantz, '"They're Coming After Us." But Who Are They Now?', *New York Times Week in Review*, 20 oktober 2002.

7 B.H. Liddell Hart, *Sherman: Soldier, Realist, American*, New York 1993, 430.

8 M. M. Lowenthal, *Intelligence from Secrets to Policy*, Washington D.C. 2003, 274.

9 K. van Kooten en W. de Bie, 'De duikboot', *Het Gat van Nederland*, 28 december 1972. Zie bijvoorbeeld S. S. Byce & R.K. Tewari, *The Anti-Submarine Warfare. Fighting the Invisible Enemy*, New Delhi 2006; J. Ukman, 'Foreign spies seeking data on underwater drones', *The Washington Post*, 3 november 2011.

No dominant adversary faces the United States that threatens our existence with military force. Rather, the complexity of the issues and multiplicity of actors – both state and non state – increasingly constitutes one of our biggest challenges.[10]

Consequenties

Wanneer een vijand uit zicht was, zo bleek in de historie sinds Sherman en Grant, kon dat ernstige consequenties hebben, gevolgen die op hun beurt tot strategische beslissingen konden leiden. Toen de Amerikaanse strijdkrachten eind november, begin december 1941 bijvoorbeeld elf dagen lang niet wisten waar de Japanse vloot voer, leidde dat tot de onverwachte aanval op Pearl Harbor, met als gevolg ruim 2400 doden, bijna 1200 gewonden, 18 uitgeschakelde schepen en bijna tweehonderd vernietigde vliegtuigen. Het betekende de entree van de Verenigde Staten in de Tweede Wereldoorlog.

Nadat de Verenigde Staten op 11 september 2001 plotseling waren getroffen door terroristische aanslagen op het World Trade Center in New York en het Pentagon door kort tevoren gekaapte vliegtuigen – waarbij bijna drieduizend doden vielen – aanslagen die door sommigen zijn omschreven als een 'nieuw Pearl Harbor'[11], proclameerde president Bush een langdurige *war on terror*. Deze oorlog zou volgens de president niet stoppen '*until every terrorist group of global reach has been found, stopped and defeated*'.[12]

Een elektronisch Pearl Harbor

Inmiddels is er de angst voor weer een 'Pearl Harbor', ditmaal een elektronisch Pearl Harbor, dat wil zeggen een cyberaanval of het teweegbrengen van een elektromagnetische puls met catastrofale gevolgen. Na aanvankelijke twijfel en scepsis noemen steeds meer deskundigen deze dreiging reëel.[13]

Dat levert het beeld op van enerzijds weinig manifeste dreigingen en tegelijkertijd een voortdurende toestand van algemene dreiging. Als gevolg van de *long war on terror* en nu ook de cyberdreiging leven we thans niet meer in vredestijd in de klassieke betekenis van het woord, maar in, wat wel genoemd is, een staat van para-oorlog, een situatie waarin op een ongewis moment een onbekende tegenstander zomaar opduikt, zonder voorafgaande oorlogsverklaring.[14] En die vijand of dreiging is als *sleeper*, *lone wolf* of Trojaans paard reeds onder ons. De kwestie van een vijfde kolonne is steeds minder een vraag en steeds meer een gegeven.

Factoren van onzichtbaarheid

Laat mij, zonder te beweren uitputtend te zijn, een aantal redenen noemen waarom het moeilijk is te zeggen wie of wat de vijanden en dreigingen de komende twintig jaar zullen zijn en waar die vandaan zullen komen.

Technologische ontwikkelingen

In de eerste plaats is er natuurlijk de technologische ontwikkeling. Sinds Nikola Tesla in 1898, overigens onder hoongelach, het beginsel van *remote control* aan Amerikaanse militaire autoriteiten demonstreerde,[15] heeft dit een duidelijke invloed gehad op oorlogvoering. Zoals de reeds genoemde drones laten zien: het is mogelijk geworden vanuit de leunstoel gevechtshandelingen aan de andere kant van de wereld uit te voeren.

10 D.C. Blair, *Annual Threat Assessment of the US Intelligence Committee for the Senate Select Committee on Intelligence,* Washington D.C. 2010, 45-46.

11 D.R. Griffin, *The New Pearl Harbor. Disturbing Questions about the Bush Administration and 9/11*, Morton-in-March 2004.

12 Geciteerd in R. Munck, 'Globalization and the limits of current security paradigms', D. Grenfell and P. James (eds.), *Rethinking Insecurity, War and Violence. Beyond savage globalization?*, London/New York 2009, 39.

13 I. Winkler, 'I Was Wrong: There Probably Will Be an Electronic Pearl Harbor', *CSO Security and Risk*, www.csoonline.com, 29 november 2009; Y.M. Butt, 'The EMP threat: fact, fiction, and response', *The Space Review*, 25 januari en 1 februari 2010; G. Ziezulewicz, 'Cyberdefenses not ready to handle "electronic Pearl Harbor", experts say', *Stars and Stripes*, 2 juni 2011; R. Mauro, 'The Electronic Pearl Harbor', *Front Page Magazine*, 20 september 2010; J. Linkins, 'On Bush's Watch, U.S. Suffered Its "Electronic Pearl Harbor"', *Huffington Post*, 10 november 2009.

14 Ch. Cogan, 'Hunters not Gatherers. Intelligence in the twenty-first century', L.V. Scott & P.D. Jackson (eds.), *Understaning Intelligence in the Twenty-First Century. Journey in the Shadows*, New York/London 2004, 147; B. de Graaff, '*Waterboarding, rendition, secret flights and prisons*. Verwording of verwezenlijking van inlichtingenvergaring als methode van terrorismebestrijding aan het begin van de 21e eeuw?', M. Kowalski & M. Meeder (eds.), *Contraterrorisme en ethiek*, Amsterdam 2011, 19; Vgl. R.A. Clarke & R.K. Knake, *Cyberwar. The Next Threat to National Security and what to do about it*, New York 2010, p. xi; S.L. Carter, *The Violence of Peace. America's Wars in the Age of Obama*, New York 2011, 4.

15 A. Jacobsen, *Area 51. An Uncensored History of America's Top Secret Military Base*, London 2011, 222-223.

Hetzelfde geldt voor *cyberattacks*. Dit soort technologische ontwikkelingen heeft ertoe bijgedragen dat de begrippen 'front' en 'territorium' steeds meer gedateerd zijn geworden.[16] Zolang er sprake is van een technologische voorsprong is degene die gebruikmaakt van de geavanceerde techniek nog redelijk identificeerbaar. Zo kunnen er zekere vermoedens bestaan ten aanzien van de vraag wie verantwoordelijk is voor de *Stuxnet*-worm die Iraanse nucleaire installaties bedreigde.[17] En zo zal er ook een redelijk vermoeden bestaan omtrent het daderschap achter vanuit drones afgevuurde *Hellfire*-raketten die doel treffen in Jemen of in Pakistan.

Maar technologie heeft de neiging te democratiseren in het gebruik en we leven in de *age of the amateur*, ook als het om geweldgebruik gaat.[18] Zoals president Obama in oktober 2009 ter gelegenheid van de maand van *National Cybersecurity Awareness* zei:

> *The very technologies that empower us to create and to build also empower those who would disrupt and destroy.*[19]

Bij leven en welzijn zal er een moment komen dat ergens boven Nederland een minidrone wordt gesignaleerd, waarvan volstrekt onduidelijk zal zijn wie of wat daarvoor verantwoordelijk is.[20] Net zo goed als nu al vaak niet duidelijk is van wie een cyberaanval afkomstig is en er tal van terroristische aanslagen zijn waarvan ook jaren nadien het daderschap niet met zekerheid is vastgesteld. De tijd dat daders een briefje achterlieten of zich, edelmoedig als ze waren, op de plaats van de aanslag gewillig aan de autoriteiten overgaven, ligt ver achter ons.

Toenemend aantal actoren

Dat brengt mij bij een tweede reden voor onzichtbaarheid: het aantal actoren dat geweld kan plegen neemt enorm toe doordat niet-statelijke en transnationale actoren zichzelf vermenigvuldigen. Dit draagt, in weerwil van voortgaande globalisering, bij aan een proces van mondiale fragmentatie.[21] Niet-statelijke actoren met kwade intenties kunnen zich bijvoorbeeld ontplooien in meer dan honderd – de afgelopen jaren in elk geval qua aantal redelijk stabiel gebleven – *failed states*. Deze niet-statelijke actoren organiseren zich ook steeds vaker als netwerken of netwerken van netwerken.[22]

Door hun gebrek aan hiërarchie en concentratie is het lastig zulke organisaties te detecteren of te elimineren. Het netwerk van Abdul Khadir Khan, dat zich bezighield met proliferatie van nucleaire kennis, kon bijvoorbeeld pas na vele jaren worden ontrafeld door inlichtingendiensten. Bovendien bleken delen van het netwerk door te kunnen werken nadat Khan eruit was geëlimineerd.[23] De veerkracht van amorfe netwerken blijkt telkens weer enorm. De toename van het aantal actoren in een taakomgeving in combinatie met hun mogelijkheid om autonoom relaties met anderen aan te gaan vergroot de onzekerheid van de (dreigings)omgeving sterk.[24]

Vandaag bondgenoot, morgen tegenstander

In zo'n dynamische, om niet te zeggen turbulente, omgeving kan de bondgenoot van vandaag gemakkelijk de tegenstander van morgen zijn, een fenomeen dat bekend is geworden als *blowback*.[25] De meest aansprekende verschijning ervan zijn waarschijnlijk de *mudjahedien* van het type Osama bin Laden, die in de jaren

16 Vgl. B. Berkowirz, *The New Face of War. How War Will Be Fought in the 21st Century*, New York etc. 2003, 3; M. Steketee, 'De oorlogen van morgen', *NRC Handelsblad*, 24 december 1999.

17 Zie bijvoorbeeld M. Martijn, 'De volgende oorlog: Cybergeddon!', *Vrij Nederland*, 31 mei 2011.

18 A. Keen *The cult of the amateur. How today's internet is killing our culture and assaulting our economy*, London/Boston 2007; G. Reynolds, *An Army of Davids. How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government, and Other Goliaths*, Nashville, Tennessee, 2006, 92.

19 www.whitehouse.gov/the-press-office/presidential -proclamation-national-cybersecurity-awareness-month.

20 Vgl. S. Shane, 'Coming Soon: The Drone Arms Race', *The New York Times*, 9 oktober 2011; A. Lorenz, J. von Mittelstaedt & G.P. Schmitz, 'Are Drones Creating a New Global Arms Race?', *SpiegelOnline*, 21 oktober 2011.

21 Vgl. D. Grenfell and P. James, 'Debating insecurity in a globalizing world. An introduction', idem (eds.), *Insecurity*, pp. 4 en 14.

22 Zie bijvoorbeeld B. de Graaff, 'Winnen de *dark mobs* het van hun bestrijders?', *BenM*, jrg. 36 (2009), nr. 2, 132-139; R. Lindelauf, *Design and Analysis of Covert Networks, Affiliations and Projects*, Tilburg 2011.

23 Lowenthal, *Intelligence*, p. 262.

24 B. de Graaff, *'Kalm temidden van woedende golven.' Het ministerie van Koloniën en zijn taakomgeving, 1912-1940*, Den Haag 1997, 629; Vgl. Naumann e.a., *Strategy*, 66.

25 Ch. Johnson, *Blowback. The Costs and Consequences of American Empire*, New York 2002.

FOTO HOLLANDSE HOOGTE

Pas na vele jaren kon het netwerk van Abdul Khadir Khan (hier afgebeeld op de vlag) worden ontrafeld

tachtig van de vorige eeuw door de Verenigde Staten en Saoedi-Arabië werden gesteund in hun strijd tegen de Russische troepen in Afghanistan, en zich daarna tegen deze landen keerden.

Maar het is een veel algemener verschijnsel. Tot aan de aanslagen van 11 september 2001 had het Westen eeuwenlang geweld geëxporteerd naar andere delen van de wereld. '9/11' markeerde het eind van dit eenrichtingsverkeer. De wereld wordt meer en meer een ricochetsamenleving, waarin elke kogel die je afvuurt vanuit een onverwachte hoek ook een keer bij je terugkomt.[26]

Robotisering

Niet alleen statelijke en sub- en transstatelijke structuren veranderen. Ook de strijders veranderen. We staan nog maar aan het begin van de robotisering, maar de komende jaren zal dit proces met rasse schreden vorderen. Ook hier is nog sprake van een technologische voorsprong van het Westen, maar deze zal eveneens als gevolg van kopiëring, *reverse engineering* of anderszins teloorgaan, zodat niet valt uit te sluiten dat de huidige generatie cadetten, als zij lang genoeg werkzaam blijven in het militaire beroep, ooit met robots als tegenstanders geconfronteerd zullen worden.[27]

We weten nog weinig over de psychologie en emoties van robots. Zullen robots emotieloze *killers* zijn of gaan we emotieve en ethische architecturen inbouwen in robots? Hoeveel erger – of minder erg – is trouwens een emotieloze killer dan een emotievolle killer?[28]

26 Vgl. M.V. Rasmussen, *The Risk Society at War. Terror, Technology and Strategy in the Twenty-First Century*, Cambridge/New York 2006, 133-135.

27 P.W. Singer, *Wirred for War. The Robotics Revolution and Conflict in the 21st Century*, London 2010; T. Weiner, 'New Model Army Soldier Rolls Closer to Battle', *The New York Times*, 16 februari 2005.

28 R.C. Arkin, 'The Case for Ethical Autonomy in Unmanned Systems', *Journal of Military Ethics*, vol. 9 (2010) no. 4, 332-341; R. Sato, 'Will Robots Evolve to Ask: "What is Life?"', *The Daily Galaxy*, 11 mei 2010; J. Mick, 'New Navy-Funded Report Warns of War Robots Going "Terminator"', *Daily Tech*, 17 februari 2009; J. Palmer, 'Call for debate on killer robots', *BBC News*, 3 augustus 2009; 'Call for debate on robot ethics', *The Independent*, 21 augustus 2009.

Mens-machine

Maar ook de mens verandert. De interactie tussen biologische en machinale componenten wijzigt razendsnel. Het zogeheten moment van *singularity*, dat is het moment waarop het onderscheid tussen mens en machine wegvalt, zal misschien niet zo snel komen als de grote protagonist van dit idee Ray Kurzweil verwacht, namelijk binnen enkele decennia, maar de ontwikkeling tendeert beslist in die richting.[29]

Ook zonder die machinale ontwikkeling zal door de biotechnologie de levensduur van de mens binnenkort snel worden verlengd. Bij een puur lineaire ontwikkeling ligt een levensduur van 150 jaar binnenkort voor de hand. Van een gemiddelde levensverwachting van iets meer dan twintig jaar rond 1800 zijn we in West-Europa gegaan naar een gemiddelde levensverwachting van rond de veertig rond 1900, en van bijna tachtig rond 2000.
Die 150 zit er sowieso in. Maar omdat de ontwikkelingen op dit gebied niet meer lineair verlopen maar exponentieel, liggen een nog hogere leeftijd en in principe onsterfelijkheid binnen ons bereik.[30] We hebben nog geen notie van hoe dit ons denken over leven en dood, en daarmee ook over geweld en oorlog, gaat veranderen. Evenmin weten we iets over de ongelijkheden die dit zal creëren als dit proces zich, zoals verwacht mag worden, niet gelijkmatig over de aardbol voordoet.[31]

De onzichtbaarheidsparadox

Een andere factor voor de moeilijke traceerbaarheid van vijanden en dreigingen zou de onzichtbaarheidsparadox kunnen worden genoemd. Waar eens kastelen en forten het landschap bepaalden, leeft nu het besef dat voor zichtbaarheid soms een hoge prijs moet worden betaald en dat onzichtbaarheid dus de beste verdediging is.[32]

We leven in het tijdperk van de bekeken mens, in de dubbele betekenis van het woord. Overal kan de mens worden bespied, maar steeds meer zal hij daar rekening mee houden, bijvoorbeeld door zich te verbergen, camoufleren, et cetera. Dat geldt evenzeer voor militairen als voor burgers. In deze transparant geachte wereld konden schurken als Karadzic, Mladic en Osama bin Laden jarenlang onder de radar en buiten beeld blijven. Er is dus zoiets als een onzichtbaarheidswedloop: hoe meer we kunnen zien, met behulp van satellieten en andere opsporingstechnieken, hoe onzichtbaarder vijanden en hun wapensystemen worden.

Miniaturisering

Dat proces wordt natuurlijk nog in de hand gewerkt door miniaturisering, zoals in het geval van de nanotechnologie, die het mogelijk maakt chips en robotjes te ontwikkelen ter grootte van een bloedcel.[33] Dat brengt bovendien de mogelijkheid met zich mee dat de vijand reeds in ons lichaam is binnengedrongen voordat wij er weet van hebben. Daar zijn verschillende mogelijkheden voor. Er wordt bijvoorbeeld nu al aandacht besteed aan het beslist niet denkbeeldige gevaar van het *hacken* van medische implantaten.[34] Hoe meer machinale onderdelen in het menselijk lichaam worden aangebracht, hoe groter dus ook de mogelijkheid tot ongewenste manipulatie, al is het maar door een stel verveelde tieners.

Verspreiding van virussen en bacteriën

Verder valt er natuurlijk te denken aan de al dan niet bewuste verspreiding van virussen en bacteriën. Ook bij deze 'onzichtbare dreiging'[35]

29 R. Kurzweil, *The Singularity is Near. When Humans Transcend Biology*, London 2005; Ch.L. Magee & T.C. Devezas, 'How many singularities are near and how will they disrupt human history?', *Technological Forecasting& Social Change*, vol. 78 (2011), 1365-1378; C. Briseno & C. Seidler, 'Researchers Hope to Build a Brain', *SpiegelOnline*, 13 mei 2011; T. Broekhuisen, 'Mens en machine groeien dichter naar elkaar toe', *Metro*, 27 augustus 2008; N. Korteweg, 'Breinbediening', *NRC Handelsblad*, 14 november 2009; R. Tomesen, 'De dag dat de computer wint', *Dagblad De Pers*, 30 oktober 2009; J. Markoff, 'Scientists Worry Machines May Outsmart Man', *The New York Times*, 26 juli 2009.

30 L. Kortekaas, 'Wetenschappers zien nog geen eind aan stijging mensenleeftijd', *Algemeen Dagblad*, 4 februari 2010; 'Scientists stop the ageing process', *ABC Science*, 11 augustus 2008; F. Macrae, 'Forever young: The pill that will keep you youthful by preventing the ills of old age', *MailOnline*, 11 juni 2011; 'De mens kan 1000 jaar worden', *De Telegraaf*, 5 juli 2011.

31 Vgl. B. Kunstler, 'Leadership in the Era of the Human Singularity: New Demands, New Skills, New Response', *The Proteus Monograph Series*, vol 2, no. 4, oktober 2008.

32 Vgl. Berkowitz, *Face*, 20.

33 Vgl. F. Simonis & S. Schilthuizen, *Nanotechnology innovations for tomorrow's defence*, Den Haag 2006.

34 'The next hacking frontier your brain?', *CNN*, 10 juli 2009.

35 A.D.M.E. Osterhaus, *Een onzichtbare dreiging in een nieuw tijdperk*, Haarlem 2001. Zie ook J. Stern, *The Ultimate Terrorists*, Cambridge, MA/London 1999; P. Kohler, *L'enNemi invisible. Notre prochain cauchemar: le bioterrorisme*, Paris 2002; G.E. Schweitzer, *A Faceless Enemy. The Origins of Modern Terrorism*, Cambridge, MA, 2002.

kan de eventuele dader zeer moeilijk te traceren zijn, zoals bijvoorbeeld bleek met betrekking tot de miltvuurbrieven in de VS in het kielzog van de aanslagen van 11 september 2001. Na bijna zeven jaar werd vastgesteld dat de vermoedelijke dader een gefrustreerde antrax-onderzoeker was van het Amerikaanse leger, die inmiddels zelfmoord had gepleegd.

Hij zou model kunnen staan voor wat genoemd wordt *super-* of *hyper-empowered* individuen,[36] mensen die (vrijwel) in hun eentje zeer grote schade kunnen aanrichten en die, juist omdat zij (bijna) alleen opereren, een ware nachtmerrie vormen voor veiligheids- en beveiligingsinstanties.

Hun optreden kan zich desgewenst ook uitstrekken tot de financiële sfeer. De afgelopen maanden is trouwens weer eens gebleken dat zich ook zonder hyper-empowered individuen financiële en economische crises kunnen voordoen, mede beïnvloed door stemmingmakerij en speculatieve transacties.

Zwermpjes

Over onzichtbare dreigingen gesproken: er komt geen met het oog waarneembare mobilisatie of logistieke verplaatsing aan te pas. De vijand komt in pakketjes, in zwermpjes die convergeren op één doel, of het nu gaat om financiële transacties, om terroristen of om *foglets*, kleine robotjes die pas op een gewenst moment een bepaalde structuur aannemen. Het falen van de Amerikaanse inlichtingen- en veiligheidsdiensten voorafgaand aan de aanslagen van 9/11 is onder meer toegeschreven aan het onvermogen *to connect the dots*, de losse onderdelen met elkaar in verband te brengen. Dit type falen belooft zich in de toekomst nog vaak te herhalen, als de vijand steeds meer in staat zal blijken zich als dots te verplaatsen.

Science fiction?

Klinkt u dit allemaal misschien als science fiction in de oren, geen nood. Met het naderen van het moment van singularity komt ook een eind aan ons vermogen ons een voorstelling van de toekomst te maken. Die zal namelijk letterlijk en figuurlijk ons verstand te boven gaan.

Voor het moment is de toegenomen onzichtbaarheid van de vijand in elk geval ook nog een gevolg van sociale constructie. We creëren ook onze nieuwe, moeilijk waarneembare vijanden en diffuse dreigingen. Steeds minder vertrouwen overheden hun eigen burgers. We bewegen ons in de richting van *surveillance states*. Om slechts twee voorbeelden te geven: direct na de aanslagen van 9/11 richtten de 'grote oren' van de Amerikaanse afluisterdienst NSA, die traditioneel altijd naar buiten waren gericht, zich op het eigen land, en Britse en Amerikaanse drones vliegen binnenkort niet uitsluitend meer boven vijandelijk gebied, maar ook – voorzien van steeds meer sensoren – boven het eigen territorium.[37]

Ook de proclamatie van een mondiale liberaal-humanitaire standaard en de eis dat gebieden zich niet mogen afsluiten maar interconnectiviteit moeten vertonen, creëert vanzelf nieuwe (potentiële) vijanden.[38] En omdat we leven in een wereld die risico's steeds minder aanvaardt en er derhalve een veiligheidsindustrie is ontstaan die de snelst groeiende economische sector van het eerste decennium van deze eeuw was, is er ook een institutioneel en op concurrentie gebaseerd belang ontstaan om telkens nieuwe vijanden te zien die voor anderen nog onzichtbaar waren.[39]

Samenzweringstheorieën

Ten slotte neemt het aantal onzichtbare vijanden nog eens toe doordat het aantal samenzweringstheorieën in het huidige tijdsgewricht sterk

36 Th. L. Friedman, *The Lexus and the Olive Tree*, New York 2000, 14-15, 140, 192, 211, 269, 398 en 462; S. Gaycken, *Cyberwar. Das Internet als Kriegsschauplatz*, München 2011, 195.

37 Vgl. J. Bamford, 'Post-9/11, NSA "enemies" include us', Politico.com, 8 september 2011; J. Lewis, 'Superspy in the sky could soon be patrolling over British cities to search for hidden terror cells', *MailOnline*, 26 april 2010; 'New drone listens in on cell phone calls and hacks Wi-Fi networks', *Homeland Security News Wire*, 5 augustus 2011.

38 Zie bijvoorbeeld Th. P. M. Barnett, *The Pentagon's New Map. War and Peace in the Twenty-first Century*, New York 2004. Voor kritische beschouwingen zie: B. de Graaff, 'Tegenbeeld en evenbeeld. Westerse interventies in falende staten toen en nu', M. Bloembergen en R. Raben (eds.), *Het koloniale beschavingsoffensief. Wegen naar het nieuwe Indië*, 1890-1950, Leiden 2009, 295-319; Rasmussen, *Risk Society*, 2-3; M. Phythian, 'Intelligence theory and theories of international relations. Shared worlds or separate worlds?', P. Gill, S. Marrin & M. Phytian (eds), *Intelligence Theory. Key questions and debates*, London/New York 2009, 65.

39 Vgl. Bamford, 'Post-9/11'.

groeit. We hebben uit het recente verleden diverse voorbeelden die laten zien hoe langs die weg nieuwe vijanden kunnen worden gecreëerd, van 'joodse plutocraten' in nazi-Duitsland tot bijvoorbeeld etnische tegenstanders met genocidale bedoelingen in voormalig Joegoslavië. En zoals de ervaring in de oorlog in Bosnië leerde: de eerste keer volstond een gerucht over vermeende activiteiten of plannen van de andere partij om strijd te ontketenen. Vervolgens hield het conflict zichzelf in een patroon van actie en reactie brandend.

Hoe sneller ontwikkelingen als automatisering of globalisering zullen gaan en hoe minder mensen het gevoel zullen hebben daar vat op te krijgen, des te groter de kans dat zij zich aan samenzweringstheorieën en dus aan onzichtbare vijanden zullen overgeven.[40]

Op spokenjacht?

In weerwil van de onzekerheid over vijanden en gevaren leidde zowel de dreiging van terrorisme als die van cyberattacks ertoe dat er strategieën zijn of worden ontwikkeld waarbij westerse mogendheden hun vijand over de hele wereld najagen. President Bush ging ervan uit dat de vijand kon worden gevonden:

> *We must take the battle to the enemy, disrupt his plans and confront the worst threats before they emerge.*

Of, zoals hij in zijn toespraak in 2002 op West Point zei:

> *We must be ready to strike at a moment's notice in any dark corner of the world.*[41]

Dat gold voor strijdkrachten; het gold ook voor inlichtingen- en veiligheidsdiensten met hun *early warning*-missie. Die moesten aan '*forward defense*' gaan doen[42] en hun medewerkers moesten veranderen van *gatherers* in *hunters*.[43] Ze moesten fysiek op zoek naar vijanden en hun habitat. En tegelijk moesten ze de zogeheten *root causes* vaststellen op basis waarvan mensen vijanden werden, zoals armoede, grondstoffentekorten, etnische tegenstellingen, mensenrechtenschendingen, de effecten van klimaatverandering, et cetera.[44]

FOTO REUTERS

President Bush ging er tijdens toespraak op West Point (2002) vanuit dat de vijand kon worden gevonden: 'We must take the battle to the enemy…'

'Grand Strategy'

Sommigen wilden op grond van al die verzamelde informatie tot een nieuwe wereldomvattende *grand strategy* komen. De afgelopen jaren gaven er diverse voorbeelden van te zien: de *global war on terror* (GWOT), de *global counterinsurgency* (GCOIN), de *Long War*, et cetera, waarbij vaak omwille van het op één noemer brengen de oorspronkelijke aan-

40 Zie ook B. de Graaff, *Op weg naar Armageddon. De evolutie van fanatisme* (te verschijnen in 2012).

41 'President Bush Delivers Graduation Speech at West Point', 1 juni 2002, http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html.

42 B. de Graaff, 'Onze cowboys in Verweggistan. De AIVD en het buitenland', De Groene Amsterdammer, 4 augustus 2010, 12-15.

43 Cogan, 'Hunters'.

44 Vgl. Naumann e.a., *Strategy*, p. 102.

dacht voor lokale en regionale onderscheiden dreigde te verdwijnen.[45]

Vermeende dreigingen

Anderen meenden dat in het licht van de ernst van sommige dreigingen er geen tijd was voor uitgebreide inventarisaties. Zij waren ongeduldiger, zoals de toenmalige Amerikaanse vicepresident Dick Cheney, die de zogeheten eenprocents-doctrine ontwierp. Deze stelt dat als er één procent kans is op een (nucleaire) dreiging van een terroristische groepering, de Amerikaanse regering daarop moet reageren '*as a certainty in terms of our response*', een leerstuk dat is omschreven als '*prevention based upon suspicion*'.[46]

Deze doctrine is wel heel extreem, maar zij is uitvloeisel van een toegenomen algemene neiging om, terwijl de vijand en de dreiging onvoldoende bekend zijn, tot de aanval over te gaan. '*Absolute proof cannot be a precondition for action*', hield de toenmalige Amerikaanse minister van Defensie Donald Rumsfeld op 6 juni 2002 de NAVO-partners in Brussel voor.[47] De marktwaarde van de woorden *pre-emptive strike* en 'preventieve oorlogvoering' is het afgelopen decennium onbetwistbaar gestegen.[48]

De oorlog ten aanzien van Irak, mede wegens de vermeende dreiging van massavernietigingswapens, liet evenwel zien hoe gemakkelijk het jagen op vijanden en dreigingen onder zulke omstandigheden kan uitlopen op het najagen van spoken en fantomen. Het laatste waar we op zitten te wachten in een wereld vol onzekerheid zijn moderne vormen van donquichotterie.

Cyberspace als nieuw slagveld

We zien nu dus een combinatie van ten eerste minder zichtbare dreigingen en ten tweede een neiging sneller toe te slaan, met alle ingebakken risico's van dien. Dit probleem is, ten derde, nog groter geworden doordat we het punt van totale globalisatie zijn genaderd. Dat wil zeggen het moment waarop afstand en geografie er niet of nauwelijks meer toe doen, niet alleen voor onszelf maar ook voor onze tegenstanders. De tijden waarin men zich erover kon verheugen dat zijn pijlen of kanonnen verder schoten dan die van de tegenstander zijn ten dele al achterhaald. En, ten vierde, hoe ver we ook op de aardbol van elkaar verwijderd zijn, we zijn tegelijk ook minder dan enkele nanoseconden van elkaar weg.

Deze combinatie van ontwikkelingen manifesteert zich op dit moment in de zich ontplooiende westerse cyberstrategieën, die ik verder als verbijzondering zal behandelen van de combinatie van onbekende dreigingen en mogelijk verkeerd gerichte daadkracht. Juist wegens de snelheid waarmee alles in cyberspace heen en weer flitst en omdat daar geen territoriale grenzen zijn, ontstaat algauw de neiging om te pleiten voor offensieve actie teneinde de vijand schade toe te brengen of zelfs te vernietigen. Hetzij door hem een koekje van eigen deeg te bezorgen, hetzij door terugbetaling in een andere muntsoort.[49] Aanval zou de beste verdediging zijn, of kunnen dienen ter afschrikking of vergelding.[50]

Bij de bekendmaking van de Amerikaanse cyberstrategie bijvoorbeeld, verklaarde de *Deputy Secretary of Defense* William Lynn dat de Amerikaanse strijdkrachten bij een cyberaanval, ook op een particulier object, zouden kunnen reageren met een '*proportional and justified military response*'.[51] Om diverse redenen is zo'n westerse cyberaanval problematisch, en dan laat ik juridische overwegingen nog buiten

45 Bijvoorbeeld Naumann e.a., *Strategy*. Vgl. R.M. Cassidy, *Counterinsurgency and the Global War on Terror. Military Culture and Irregular War*, New York 2006; M.C. Meigs, 'Unorthodox Thought about Asymmetric Warfare', *Parameters*, Summer 2003, 14.

46 R. Suskind, *The One Percent Doctrine. Deep Inside America's Pursuit of Its Enemies Since 9/11*, London 2007, 62, 150, 163-170.

47 Geciteerd in P. James and J. Friedman, 'Globalization and the changing face of war', Grenfell and James (eds.), *Rethinking*, p. 30. Cheney drukte zich in dezelfde termen uit, Carter, *Violence*, 31.

48 Zie bijvoorbeeld Berkowitz, *Face*, 8; Carter, *Violence*, 20.

49 Vgl. Clarke, *Cyyber War, pp. 45-46*.

50 De Amerikaanse National Strategy for Cyber Operations, geciteerd in Clarke, *Cyber War*, 45; 'Pentagon considers preemptive strikes as part of cyber-defense strategy', *The Washington Post*, 31 augustus 2010; *Department of Defense Strategy for Operating in Cyber Space*, juli 2011, 7; 'We'll strike first in cyber warfare. Hague sends enemies warning', *The Sun*, 18 oktober 2011; M.A.D. Tetteroo & P. de Graaf, 'Het vijfde domein van de krijgsmacht', *Militaire Spectator* 179 (2010) (5) 248; P.A.L. Ducheine & J.E.D. Voetelink, 'Cyberoperaties: naar een juridisch raamwerk', *Militaire Spectator* 180 (2011) (6) 277; L. Essers, 'Nederlands cyberleger kiest ook voor de aanval', *Webwereld*, 14 november 2011.

51 J.N. Hoover, 'U.S. Military Outlines Cyber Security Strategy', *InformationWeek*, 14 juli 2011.

beschouwing.[52] Ten eerste is de identiteit van (potentiële) daders in cyberspace vaak nog lastiger vast te stellen dan op andere terreinen.[53] Het is daarmee goed mogelijk bij cyberacties onder valse vlag te opereren en daarmee ongerechtvaardigde aanvallen uit te lokken. Als we al wel een vermoeden hebben van de identiteit van de dader, dan zou juist dat ons weleens kunnen weerhouden van offensieve actie. Bijvoorbeeld omdat in menig geval de tegenstander zijn defensie beter op orde heeft of minder afhankelijk is van cyberspace dan westerse landen.[54] Voor zover er sprake kan zijn van afschrikking in cyberspace is de kans dat die zich tegen ons richt dan ook groter dan dat die in ons voordeel werkt.

Maar stel dat westerse landen overgaan tot offensieve cyberoperaties, dan is er een ernstig risico van *collateral damage*.[55] De Stuxnet-worm bijvoorbeeld had wereldwijde neveneffecten en had ook in Nederland gevolgen. Bovendien ontstond naar aanleiding van deze worm de vrees dat zoiets zou kunnen worden overgenomen door hackers.[56] Er moet dan ook beslist niet worden blindgestaard op de *capabilities* van eigen offensieve acties in cyberspace, omdat daarmee de strategische doelen en belangen wel eens uit het oog verloren zouden kunnen raken.[57] Bovendien zou door dit soort acties het karakter van een staat van para-oorlog nog veel sterker kunnen worden aangezet.

De legitimiteitskwestie

Dat brengt mij ten slotte bij de kwestie van de politieke legitimiteit. Is het erg dat de vijand, hoe dan ook, buiten beeld raakt? Het antwoord luidt: ja. Opereren tegen een onzichtbare vijand kan gedurende zekere tijd door burgers worden aanvaard, zeker wanneer er sprake is van angst of van een angstpsychose. Op den duur holt het fantoomkarakter van de vijand en/of het voortdurend opereren buiten het gezichtsveld van de burgers echter de legitimiteit van het eigen optreden uit. Herstel van zekerheid[58] is een illusie; we moeten leren leven met onzekerheid – dat geldt zeker voor de militair[59] – en daarover ook communiceren met het publiek. Leven met risico's vereist een open debatcultuur.[60]

Geheime oorlogen

De vraag is dus niet alleen: welke vijand is onzichtbaar, maar ook: voor wie is de vijand onzichtbaar? Anders gezegd, worden er oorlogen uitgevochten die voor een breder publiek verborgen blijven, terwijl strijdkrachten en inlichtingen- en veiligheidsdiensten daar wel van op de hoogte zijn? In algemene zin is het antwoord gemakkelijk te geven: er was het afgelopen decennium herhaaldelijk sprake van *secret flights*, *secret prisons* en *secret wars*. De inzet van drones is vaak onderdeel van schimmige deals met schimmige regimes.[61] Democratische principes en geheimhouding verdragen elkaar slecht. Het zal niet gemakkelijk zijn bij geheime oorlogen de balans tussen geheimhouding en democratische waarden te bewaren.[62]

Draagvlak

Als mensen blijvend het gevoel hebben dat ze oorlogen worden 'ingerommeld' of dat er van de aard van de militaire inzet een verkeerd beeld wordt geschetst, doet dat afbreuk aan het draagvlak voor de strijdkrachten. En wat bovenal afbreuk aan legitimiteit zou doen, zou een situatie zijn waarin burgers het idee krijgen dat er offensieve acties worden uitgevoerd die ten koste gaan van de verdediging van hun directe belangen. Op het terrein van cyberdefensie is er zoveel mis, bij particulieren, bij overheden en, helaas, niet zelden ook bij defensieorganen en inlichtingen- en veiligheids-

52 Zie daarvoor Ducheine & Voetelink, 'Cyberoperaties'.
53 Clarke, *Cyber War*, xi, 214; Lowenthal, *Intelligence*, 258, 273; S. Gorman, 'Electricity Grid in U.S. Penetrated by Spies', *The Wall Street Journal*, 8 april 2009; Ducheine & Voetelink, 'Cyberoperaties', 282; J. Markoff, D.E. Sanger & T. Shanker, 'In Digital Combat, U.S. Finds No Easy Deterrent', *The New York Times*, 26 januari 2010.
54 Vgl. Clarke, *Cyber War. The Next Threat to National Security and What to do about it*, New York 2010, xiii, 27, 105-106, 145-148, 194-196, 217.
55 E. Nakashima, 'Pentagon: Offensieve cyber attacks fair game', *The Washington Post*, 15 november 2011; Clarke, *Cyber War*, p. 202.
56 J. Markoff, 'A Silent Attack, but Not a Subtle One', *The New York Times*, 26 september 2010; A.U. de Haes, 'Stuxnetworm valt Nederlands bedrijf aan', *Webwereld*, 4 oktober 2010.
57 C.S. Gray, *National Security Dilemmas. Challenges & Opportunities*, Washington D.C. 2009, 6-8.
58 Naumann e.a. *Strategy*, 148.
59 Vgl. A. Bousquet, *The Scientific Way of Warfare. Order and Chaos on the Battlefields of Modernity*, London 2009, 242.
60 Vgl. Rasmussen, *Risk Society*, 4.
61 Zie bijvoorbeeld Jacobsen, *Area 51*, 352-353.
62 Vgl. Berkowitz, *Face*, xii.

FOTO REUTERS, R. WILKINS

Op het terrein van cyberdefensie is op allerlei niveaus veel mis

diensten,[63] dat er beter daarop kan worden geconcentreerd dan op spannende, maar mogelijk contraproductieve offensieve plannen. We moeten voorkomen dat we in een situatie terechtkomen die vaak het Nederlandse voetbal kenmerkt: aantrekkelijke aanvallen, maar een verwaarlozing van de defensie, waardoor de grote slagen altijd verloren gaan.

Schijnaanvallen

Preventieve bescherming op het thuisfront moet, in het bijzonder op het terrein van cyber, de basis zijn van elke toekomstige strategie. Dat wil zeggen minimalisering van de kwetsbaarheid, minimalisering van de schade en optimalisering van de herstelcapaciteit.[64]

Ik zou daarom een sterk pleidooi willen houden voor cyber-*red teams*, die voortdurend (schijn)aanvallen uitvoeren op de eigen systemen om deze te testen op hun weerbaarheid.[65] Daarmee kunnen we hopelijk grotendeels voorkomen dat anderen dan wijzelf de *trial runs* ten aanzien van onze cybersecurity doen.

De beste verdediging is dan dus de oefenaanval,[66] met bovendien dit voordeel dat we dan tenminste weten wie de vijand is en ook hoe onze eigen systemen ervoor staan. Daarmee volgen we een al bijna drie millennia oude les van de Chinese strateeg Sun Tzu:

> *Wanneer u uw vijand niet kent, maar u kent uzelf, dan zijn uw kansen om te winnen of verliezen gelijk. Indien u noch uw vijand noch uzelf kent, dan loopt u zeker in elke slag gevaar.*[67]

Ten slotte

Wellicht waren Sherman en Grant dan toch moderner dan ik ze aan het begin van dit verhaal afschilderde. Misschien valt er veel voor te zeggen om je niet al te druk te maken voordat vijanden zich manifesteren, want voor je het weet heb je er een paar extra in het leven geroepen of verzonnen.

Het is mij niet gegeven thans dieper in te gaan op de punten die ik heb aangesneden. Ik hoop niettemin dat ik genoeg overhoop heb gehaald om u aan het denken en debatteren te zetten over de toekomst van dreiging en conflict, iets wat naar mijn smaak niet beter kan gebeuren dan aan een militaire academie.

Tot de cadetten, maar niet alleen tot hen, zou ik willen zeggen: ik hoop dat uit het voorafgaande duidelijk is geworden dat in de toekomst meer dan ooit behoefte bestaat aan intellectueel ontwikkelde militairen. En om na al deze onzekerheden te eindigen met een vaststaand gegeven: er zal dit komende jaar en de vele die er nog op zullen volgen aan deze academie hard worden gewerkt aan deze intellectuele ontwikkeling en ontplooiing. En ik wens u daarbij veel inspiratie en debat toe. ■

63 Zie bijvoorbeeld B. de Winter, 'Iran kan Gmail aftappen door Nederlands certificaat', *webwereld*, 29 augustus 2011; idem, '14 staatsbedreigende aanvallen in 2 jaar', *webwereld*, 15 september 2011; 'Defense official discloses cyberattack', *The Wahington Post*, 24 augustus 2010; 'Cyber attack on France targeted Paris G20 files', *BBC News*, 7 maart 2011; A. Nguyen, 'Foreign Office blocked "significant" cyber attack, says GCHQ chief', *Computer World UK*, 31 oktober 2011; 'MI5 inspector's website shut down after security blunder', *The Telegraph*, 23 oktober 2011; 'Sacre bleu! French snooped on British government emails', *Security Watchdog*, 27 oktober 2011; J. Schellevis, 'Terrorismebestrijder: reactie overheid op DigiNotar niet adequaat', *tweakers.net*, 15 november 2011; *Department of Defense Strategy for Operating in Cyber Space*, juli 2011, 4.

64 Vgl. Naumann e.a., *Strategy*, 99.

65 *Department of Defense Strategy for Operating in Cyber Space*, juli 2011, 5.

66 Vgl. Defensiewoordvoerder M. Hilbrandie in L. Essers, 'Cyberleger'.

67 Sun Tzu, *The Art of War*, London etc. 1971, 84.