

MILITAIRE SPECTATOR



De Belfast flag issue

- Vaandelopschrift Koninklijke Luchtmacht voor Allied Force
- Cybersecurity: trends voor Defensie

AANKONDIGING

KVBK field trip

19 april 2013 - Vught

De KVBK organiseert dit jaar in plaats van een battlefield tour voor het eerst een field trip.

Dit nieuwe concept maakt het mogelijk om één maal per jaar een themadag aan te bieden die actuele zaken binnen de krijgsmacht koppelt aan krijgswetenschappelijke (historische) onderwerpen. Per krijgsmachtdeel zal dit rouleren en als eerste komt het Commando Landstrijdkrachten aan de beurt.

Het programma biedt een combinatie van actuele ontwikkelingen op het gebied van civiel-militaire samenwerking bij C-IED en CBRN en een historische wandeling van circa vijf kilometer in de omgeving van Kamp Vught. Deskundigen verzorgen inleidingen en tevens zijn er demonstraties.

De KVBK field trip vindt plaats op vrijdag 19 april 2013 in en om het Huis van het regiment Genietroepen (Geniemuseum) aan de Lunettenlaan 102 in Vught. Om 09.00 uur worden de deelnemers verwelkomd met koffie, waarna het programma om 10.30 uur begint. De field trip duurt tot circa 17.00 uur en is inclusief lunch.

Geïnteresseerden kunnen zich tot vrijdag 5 april per e-mail opgeven bij de secretaris van de KVBK, majoor van de Koninklijke Luchtmacht Daan Storm van Leeuwen: secretaris@kvbk.nl.

De inschrijving sluit bij zestig deelnemers. Deelname is gratis voor leden van de KVBK.

Voor niet-leden zijn de kosten tien euro.

Nadere informatie, waaronder een routebeschrijving, parkeertips, betaalwijze en een gedetailleerder programma, is te vinden op www.kvbk.nl en op www.facebook.com/KVBKNederland.





MILITAIRE SPECTATOR

UITGAVE

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

Secretaris en ledenadministratie

Majoor Daan Storm van Leeuwen
DM.StormVanLeeuwen@mindef.nl

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

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

REDACTIE

brigade-generaal cav b.d. prof. em.
J.M.J. Bosch (hoofdredacteur)
T 071 - 542 18 30
E jmjbosch@xs4all.nl
kolonel cav drs. P.J.E.J. van den Aker
kolonel KLu S.M. Babusch bc
kapitein ter zee P. van den Berg
drs. P. Donker
kolonel MJD dr. P.A.L. Duchaine
luitenant-kolonel MPSD dr. J. Ducl
cdre KLu b.d. F. Groen
drs. P.H. Kamphuis
luitenant-kolonel KMar drs. ing. D.J. Muijskens
luitenant-kolonel Mams dr. drs.
A.J.E. Wagemaker MA
kapitein ter zee mr. N.A. Woudstra
kolonel ir. F.J.A. van Zitteren

BUREAU REDACTIE

mw. drs. A. Kool
dr. F.J.C.M. van Nijnatten
NIMH
Postbus 90701
2509 LS Den Haag
T 070 - 316 51 20 of
070 - 316 51 95
E redactiemilitairespectator@mindef.nl

De Militaire Spectator is aangesloten bij
de European Military Press Association

LIDMAATSCHAP

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

OPMAAK EN DRUK

Drukkerij ten Brink
ISSN 0026-3869
Nadruk verboden

Coverfoto: Demonstratie van Noord-Ierse
loyalisten bij City Hall in Belfast,
december 2012
(Foto Foto ANP, P. Muhly)

112 'Belfast flag issue' en de kwetsbare vrede in Noord-Ierland

Th.B.F.M. Brinkel en J.E. Noll

Als etnisch en religieus verdeelde regio is Noord-Ierland een belangrijke casus voor onderzoek naar verzoening en wederopbouw en ook voor de Nederlandse krijgsmacht liggen er lessen over stabilisatie-operaties.

125 Onderzoek naar *Allied Force* staft toekenning vaandelopschrift Koninklijke Luchtmacht

J. Müller en R. de Winter

Aan de toekenning van een vaandelopschrift aan de Koninklijke Luchtmacht voor de inzet tijdens *Allied Force* ging een onderzoek vooraf waarvan de bevindingen de collectieve onderscheiding rechtvaardigen.

136 Cybersecurity: relevante trends voor Defensie

H.J. van der Molen

Defensie moet beschikken over voldoende cyberkennis om het risico van cyberaanvallen voor de eigen installaties te verminderen en om mee te kunnen denken over de bescherming van Nederlandse (civiele) vitale systemen.

En verder:

Editoriaal	110
Andere ogen	151
Tegenwicht	152
Boeken	154
Summaries	

Nederland en de wereld

De agenda staat vol met jubilea. In 2013 vieren we een eeuw militaire luchtvaart in ons land en schenkt de Koninklijke Marine aandacht aan haar 525 jaar oude ankers. Volgend jaar is het de beurt aan de Koninklijke Landmacht en de Koninklijke Marechaussee, die dan uitgebreid stilstaan bij hun tweehonderdjarig bestaan. De rijke historie van de krijgsmachtdelen valt niet los te denken van de politieke strategie die aan hun geschiedenis ten grondslag ligt. Hoe heeft deze strategie vorm gekregen?

Lidmaatschap van de Verenigde Naties, de West-Europese Unie, de NAVO en de EU heeft Nederland geen windeieren gelegd

Begin van de vorige eeuw kende Nederland een rotsvast vertrouwen in zijn politiek van afzijdigheid en gewapende neutraliteit. Dit leek aanvankelijk te werken: de belligerenten van de Eerste Wereldoorlog eerbiedigden de Nederlandse neutraliteit. Maar in mei 1940 werd Nederland ruw uit zijn droom gewekt. Die ontnuchterende ervaring leidde na de oorlog tot een radicale koerswijziging. Nederland zocht zijn heil in internationale samenwerking en ons land behoorde tot de eerste leden van de Verenigde Naties, de West-Europese Unie, de Noord-Atlantische Verdragsorganisatie, de Europese Gemeenschap voor Kolen en Staal en de Europese Economische Unie (de voorloper van de huidige Europese Unie).

Deze lidmaatschappen hebben ons geen wind-eieren gelegd – onze welvaart en onze veiligheid hebben we als een relatief klein land met een grote, open economie in niet geringe mate aan die internationale samenwerkingsverbanden te danken.

Twee reflexen hebben bij de internationale inbedding van ons land altijd een rol gespeeld: de Europese en de Atlantische. De daarmee gepaard gaande beleidsopties zijn lange tijd als concurrerend beschouwd, maar gaandeweg is het besef ontstaan dat – ook op veiligheidsgebied – verdergaande Europese samenwerking en de trans-Atlantische NAVO-band met de Verenigde Staten elkaar niet hoeven te bijten.

Het is opvallend dat beide hoofdpunten in het Nederlandse veiligheidsbeleid van de afgelopen decennia sleetse plekken vertonen en in de publieke opinie, ook in ons land, minder enthousiasme oproepen dan vroeger het geval was. Hoewel successen in het verleden geen garantie vormen voor een geslaagde toekomst, verbaast het gemak waarmee sommigen de NAVO tot zieke, oude man verklaren of het dedain waarmee anderen de wens uitspreken om tot renationalisering van de Europese verworvenheden te willen overgaan.

Een gedegen kennis van de recente geschiedenis, van de politieke, economische en technologische ontwikkelingen in de wereld en van de voortschrijdende globalisering op tal van terreinen, lijken in het politieke discours aan belang te hebben ingeboet.

Kijken we naar de NAVO, dan moeten we constateren dat de val van de Muur grote gevolgen

heeft gehad voor onze belangrijkste verzekering op veiligheidsgebied. Een duidelijke bedreiging – ook voor de man in de straat – is weggevallen en de NAVO is razendsnel uitgebreid. Het NAVO-verdragsgebied is niet langer meer een knellend keurslijf en de NAVO is – als een van de weinig regionale veiligheidsorganisaties – in staat gebleken tot expeditionaire inzet, ook al ging de politieke besluitvorming niet altijd van een leien dakje.

De grote broer – de Verenigde Staten – is bezig met een strategische heroriëntatie en verwacht, ook om economische redenen, dat de relatief rijke Europeanen beter de eigen broek gaan op houden. De belangrijkste uitdaging voor het NAVO-huis in Brussel is het ontwikkelen van een aansprekend gemeenschappelijk perspectief op wat er onder bedreigingen van de gemeenschappelijke veiligheid moet worden verstaan, en hoe daarop ware te reageren.

Kijken we naar dat andere Brussel, dat van de Wetstraat als motor in het proces van Europese samenwerking, dan valt op hoezeer een weef fout in het Verdrag van Maastricht – de invoering van een gemeenschappelijke munt zonder overdracht van noodzakelijke bevoegdheden op het gebied van de nationale begrotingsdiscipline – heeft geleid tot een uitholling van de publieke steun voor Europa. De financiële crisis trekt diepe sporen – en de emoties bij veel slachtoffers van wanbeleid, megalomane persoonlijkheden en graaiers aan de top zijn – begrijpelijk – groot.

Toch moeten we zeker in ons land niet vergeten hoe zeer onze economische welvaart te danken is aan die gemeenschappelijke markt –

als meest in het oog springende symbool van de Europese samenwerking. Zeker, het zoeken naar een passend antwoord op die crisis van nu kost tijd; de lidstaten hebben immers verschillende uitgangspunten en specifiek nationale belangen te behartigen. Het is in dit opzicht goed dat het kabinet Rutte-Samson de ratio in de besluitvorming ten aanzien van Brussel weer heeft teruggebracht – en minder leunt op anti-Europese onderbuikgevoelens dan zijn voorganger.

Het is aan te bevelen dat in beide ‘Brussels’ ons land weer op constructieve wijze zijn partijtje mee blaast. Ook hier kan de geschiedenis als spiegel fungeren. Nederland heeft zowel bij de NAVO als de Europese Unie altijd op bekwame wijze meegesproken, en op die manier de eigen belangen behartigd. De geografische ligging, de relatief grote en sterke ‘open’ economie, consistente beleidsopvattingen, bekwame diplomaten en een geloofwaardige krijgsmacht bleken belangrijke krachtbronnen.

Bovendien was het besef aanwezig dat wie wil samenwerken, zijn partner(s) iets te bieden moet hebben. Wie thans voor een dubbeltje op de eerste rang denkt te kunnen zitten en toch volwaardig denkt te kunnen meepraten, is een naïeve optimist. Ook in het verkeer met bondgenoten en bevriende landen gaat het om het behartigen van nationale belangen – en een duidelijke visie op die Nederlandse belangen in de wereld en een goed gevulde diplomatieke én militaire gereedschapskist is dan ook geboden. ■

De 'Belfast Flag Issue' en de kwetsbare vrede in Noord-Ierland

Vlak voor kerstmis 2012 besloot de gemeenteraad van Belfast om de 'Union Jack' (de vlag van het Verenigd Koninkrijk) niet meer 365 dagen per jaar te hijsen, maar alleen op speciaal aangewezen dagen. Dat besluit gaf aanleiding tot een uitbarsting van rellen, die voor velen binnen en buiten (Noord-)Ierland als een verassing kwamen. Na het Goede Vrijdag-akkoord uit 1998, waarmee een einde kwam aan dertig jaar geweld, leek het besluit een eenvoudige beslissing waarmee Belfast zich aansloot bij de rest van het Verenigd Koninkrijk. In dit artikel gaan de auteurs in op de recent uitgebroken rellen in Noord-Ierland. Ze onderzoeken de mogelijke oorzaken ervan en kijken naar de toekomstige kansen van het vredesproces, dat kennelijk nog steeds kwetsbaar is.

*Dr. Th.B.F.M. Brinkel en dr. J.E. Noll**

Dit proces is om meerdere redenen interessant. Noord-Ierland is – als etnisch en religieus verdeelde regio – een belangrijke casus voor onderzoek naar verzoening en wederopbouw. Het is een test-case van theorieën van onder anderen Arend Lijphart over *power-sharing* (machtsdeling). Theorieën over *power-sharing* zijn ontwikkeld om vreedzaam samenleven van sterk verdeelde staten mogelijk te maken en te verklaren. Successen en mislukkingen in Noord-Ierland zijn daarnaast relevant voor het begrip van soortgelijke conflicten in andere gebieden, zoals Bosnië-Herzegovina en Kosovo.

Relevantie Nederlandse krijgsmacht

Ook voor de Nederlandse krijgsmacht kan het van belang zijn om kennis te nemen van het

Noord-Ierse vraagstuk en de recente onrust. In stabilisatieoperaties is militaire inzet ter wille van het scheppen van orde en veiligheid belangrijk. Maar voor de langere termijn zijn ook politieke regelingen nodig die recht doen aan het streven en de verlangens van de betrokken bevolking.

Dit sluit aan bij lessen die zijn getrokken in vredesoperaties, zoals in Bosnië-Herzegovina of Afghanistan, waar de NAVO en de betrokken landen een *comprehensive approach* toepassen. Daarbij werden en worden politiefunctionarissen en/of militairen ingezet voor de handhaving van veiligheid. Die inzet kan niet los worden gezien van de noodzaak rechtvaardige en democratische instellingen tot stand te brengen of te consolideren, en van de noodzaak om sociaaleconomische ontwikkeling op gang te brengen.¹

Wat in Noord-Ierland gebeurt is daarom leerszaam en relevant. Het is een gebied waar in de jaren zeventig en tachtig duizenden doden zijn gevallen in de katholieke en de protes-

* Theo Brinkel is hoofd Fundamentele Voorlichting en waarnemend sectieleider Internationale Veiligheidsstudies van de Faculteit Militaire Wetenschappen van de NLDA. Jörg Noll is als universitair hoofddocent Internationale Veiligheidsstudies verbonden aan dezelfde faculteit.

1 In de wetenschap spreekt men vaak van *sequencing* en de vraag welke volgorde belangrijker is: eerst veiligheid en dan democratische en sociaaleconomische ontwikkeling of andersom? Noord-Ierland toont aan dat het noodzakelijk is om beide processen parallel te laten plaatsvinden, omdat het anders onmogelijk is de vicieuze cirkel van geweld te doorbreken.

tantse gemeenschappen en onder Britse militairen. Er zijn ervaringen opgedaan met verzet, *counterinsurgency*, terrorisme en contraterro-risme, verzoening, vredesonderhandelingen en post-conflict wederopbouw.

Er is een nieuwe staatsregeling in het leven geroepen en de orde- en veiligheidsdiensten hebben een transformatie ondergaan opdat ze representatief zijn voor de gemeenschap waarin ze opereren. Dat zijn allemaal lessen die ook voor Nederlandse militairen relevant zijn, want die facetten komen voor in het Nederlandse beleid over wederopbouw na conflict.

Opzet artikel

Om te laten zien hoe kwetsbaar de vrede in Noord-Ierland is gaan we eerst in op de recente rellen. Voor een beter begrip van de situatie schenken we daarna aandacht aan de voorgeschiedenis en aan de theorie van power-sharing (machtsdeling), die richtinggevend is geweest bij het ontwerpen van een nieuwe constitutionele regeling.

Daarna volgt een poging het verschijnsel te verklaren. Vervolgens komen enkele politieke ontwikkelingen aan de orde die het verdere verloop van het vredesproces in Noord-Ierland kunnen bemoeilijken. Het artikel eindigt met conclusies.

De bevindingen in dit artikel zijn gebaseerd op literatuur, bronnen en op informatie uit de eerste en de tweede hand, die we onder meer tijdens een reis door Noord-Ierland en de Republiek Ierland inwonen. We waren daar persoonlijk getuige van de demonstraties.

De vlaggenkwestie

De aanleiding voor de demonstraties was het besluit van de gemeenteraad van Belfast op 3 december 2012 om de *Union Jack*, de bekende vlag van het Verenigd Koninkrijk (VK), nog maar op achttien dagen per jaar te hijsen. Dit kwam overeen met de regels die in de rest van het VK gelden. Terwijl de raad vergaderde, begonnen buiten de protesten. Velen hadden de symbolische betekenis van de vlag op het



FOTO: REUTERS

Een Britse militair tijdens de Oranjeparade in Noord-Ierland. De recente gebeurtenissen hebben duidelijk gemaakt hoe kwetsbaar de vrede nu nog steeds is

stadhuis van de hoofdstad van Noord-Ierland onderschat.

De Union Jack symboliseert de Britse identiteit en soevereiniteit, zoals Hobsbawm en Ranger schrijven.² Bovendien is uiterekend die vlag uitdrukking van de band van Noord-Ierland met de rest van het VK.³ Het ontwerp van de vlag in zijn huidige vorm is in 1801 ontstaan met de Unie van Groot-Brittannië en Ierland. De Union Jack is een combinatie van de vlaggen van Engeland, Schotland en Ierland.

Wie door de protestantse wijken van Belfast rijdt en het vlagvertoon in de straten ziet, kan duidelijk zien dat de vlag voor veel protestanten cruciaal is. Het lijkt het symbool bij uitstek van de protestanten om zich van de katholieke gemeenschap te onderscheiden.

2 Eric Hobsbawm and Terence Ranger (eds.) *The Invention of Tradition* (Cambridge: Cambridge University Press 2012) 11.

3 www.bbc.co.uk/news/uk-northern-ireland-20951202.

Compromis

Het besluit om de vlag minder dagen te hijsen was eigenlijk een compromis, in lijn met de ideeën van machtsdeling. De republikeinen/nationalisten – voorstanders van aansluiting van Noord-Ierland bij Ierland en voornamelijk katholiek – willen dat de Britse vlag helemaal verdwijnt. Unionisten – aanhangers van behoud van de band met het VK – willen de vlag behouden.

De *Alliance Party*, een van de partijen in het Noord-Ierse parlement die zichzelf noch als pro-Brits noch als pro-Iers beschouwen, had aangestuurd op het huidige besluit. Het werd gesteund door de pro-Ierse partijen. De unionisten waren tegen. In een opiniërend artikel schreef First Minister Peter Robinson, politiek leider van de *Democratic Unionist Party* (DUP, zie hieronder), dat de unionisten tegen het besluit waren, maar dat het langs parlementaire weg moet worden bestreden.⁴

Binnen enkele minuten na het besluit liepen de protesten uit de hand. Het begon met het beschadigen van ramen en auto's van raadsleden. In de dagen erna werden de protesten heviger. Vooral politici van de Alliance werden bedreigd, zozeer zelfs dat de politie hen adviseerde een veilig onderkomen te zoeken.⁵

Ook vertegenwoordigers van andere partijen werden bedreigd. Dat gold niet alleen voor de pro-Ierse partij Sinn Fein, maar ook voor de leider van de unionistische DUP, First Minister Peter Robinson. Ook zijn er tijdens de rellen honderden politiemensen gewond geraakt.

Inschattingsfout

Op 7 januari 2013 trok een groep van pakweg 250 betogers over Great Victoria Street naar het stadhuis om daar te protesteren. Het waren voor het grootste deel jongeren van rond de

twintig, maar er waren ook vrouwen met buggy's en jonge kinderen bij.⁶ Na een verhoudingsgewijs rustig protest trok deze groep richting Oost-Belfast, de oorsprong van de protestbeweging. Ze werden begeleid door de oproerpolitie, die de menigte probeerde te kanaliseren.

Nog in dezelfde nacht kwam het echter tot hevige rellen, zoals door de experts met wie de auteurs eerder op die dag spraken, was voorspeld. Binnen een week trokken meer dan duizend betogers naar het stadhuis en werden ook de rellen in het oosten van de stad heviger dan daarvoor. Blijkbaar had de oproerpolitie, die de menigte via een brug van een katholieke woonwijk weg wilde leiden, een inschattingsfout gemaakt. Zij had er namelijk niet op gerekend dat de relschoppers een andere brug namen en op die manier alsnog slaags raakten met katholieke jongeren.⁷

Het is moeilijk te achterhalen wie de onruststokers zijn en wie de demonstranten tot rellen weten aan te zetten. In de aanloop naar het besluit van de gemeenteraad hadden activisten van de protestantse partijen in het Noord-Ierse parlement de gemoederen opgestookt met het verspreiden van bijna 40.000 pamfletten. De Deputy First Minister Martin McGuinness van Sinn Fein meent dat de *Ulster Volunteer Force* (UVF, een protestantse vigilante groep) bij de organisatie van de rellen betrokken is.⁸ Ook vertegenwoordigers van de *Police Service of Northern Ireland* vermoeden dat personen uit de UVF achter de organisatie van de rellen zitten.⁹ Deze vermoedens zijn echter nog niet bewezen.

Om op zoek te gaan naar de mogelijke oorzaken van de huidige protesten is het zinvol een nadere beschouwing te wijden aan de voorgeschiedenis. Deze komt in de volgende paragraaf aan de orde.

Voorgeschiedenis

De recente ontwikkelingen moeten worden gezien tegen de achtergrond van een uiterst gewelddadige geschiedenis van Noord-Ierland.

4 www.mydup.com/news/opinion-peter-robinson-on-decision-to-remove-flag-from-belfast-city-hall.

5 www.bbc.co.uk/news/uk-northern-ireland-20720406.

6 Waarneming van de auteurs.

7 www.bbc.co.uk/news/uk-northern-ireland-21020768.

8 www.bbc.co.uk/news/uk-northern-ireland-21012524.

9 www.bbc.co.uk/news/uk-northern-ireland-20651163.

Vooral de jaren zeventig en tachtig, de zogeheten *Troubles*, kenmerkten zich door aanslagen, rellen en geweld.

In de jaren zeventig kwamen gemiddeld 275 mensen per jaar om; een gemiddelde dat in de jaren tachtig afnam naar tussen de vijftig tot honderd politieke moorden per jaar. Aan het eind van de twintigste eeuw waren rond de 3600 mensen gedood; 363 op naam van Britse veiligheidstroepen, vijf op naam van Ierse veiligheidstroepen, 1016 door toedoen van loyalistische paramilitairen, 2061 door republikeinse paramilitairen en 84 van wie de dader onbekend is.¹⁰

Nationalisten

Aan het conflict namen verschillende partijen deel. Aan de ene kant stonden de nationalisten of republikeinen, die streefden naar aansluiting van Noord-Ierland bij de Ierse Republiek. De bevolkingsgroep waar zij uit voortkwamen bestond uit katholieken, die jarenlang in Noord-Ierland werden achtergesteld in politiek, economisch en sociaal opzicht.

Het nationalistisch geweld kan vooral op het conto van de *Provisional Irish Republican Army* (IRA, *Provisionals*, *Provos*) worden geschreven.¹¹ Als de meer gematigde nationalistische partij kwam de *Social Democratic and Labour Party* (SDLP) naar voren; de meer radicale partij was *Sinn Féin*. Deze laatste was nauw verbonden met de IRA. De SDLP vond dat de aansluiting bij de Republiek op vreedzame wijze zou moeten gebeuren.

Unionisten

Aan de andere kant stonden de unionisten of loyalisten. Zij zijn protestant, vormen de meerderheid in Noord-Ierland en waren politiek, economisch en sociaal dominant. Voor hen was het vasthouden aan de band met het VK een vorm van behoud van identiteit. Het democratisch staatsbestel van het VK is voor hen nauw verbonden met de ontwikkeling van het protestantisme op de Britse eilanden.

De unionisten vreesden te veel te zullen verliezen wanneer Noord-Ierland zich zou aan-



FOTO AUTEUR

Een muurschildering van Bobby Sands, in de katholieke Falls Road wijk in Belfast. Bobby Sands is een martelaar geworden in de politieke strijd van de IRA

sluiten bij het door katholieken gedomineerde Ierland. Unionisten hadden twee grotere politieke partijen: de *Ulster Unionist Party* (UUP) en de radicalere *Democratic Unionist Party* (DUP), die lange tijd onder leiding stond van de extreem protestantse dominee Ian Paisley. Unionistisch geweld werd onder meer gepleegd door de *Ulster Volunteer Force*, eind jaren zestig heropgericht als gewapende beweging die zich inzette voor het behoud van het Britse karakter van Noord-Ierland.

De regering

De derde partij in het conflict was de regering in Londen, Westminster. Deze had het formele gezag over Noord-Ierland, maar was geneigd het Noord-Ierse vraagstuk zo veel mogelijk op afstand te houden. De openbare orde werd gehandhaafd door de politie, de *Royal Ulster Constabulary* (RUC), die werd ondersteund door de *British Army*.

10 Malcolm Sutton, Summary of organisation responsible for the death, *An Index of deaths from the conflict in Ireland*, CAIN webservice, http://cain.ulst.ac.uk/sutton/tables/Organisation_Summary.html.

11 De Provisional IRA is in 1969 afgesplitst van de IRA, die in de jaren zestig een marxistische koers was gaan varen. De Provisionals zijn sindsdien de hoofdstroom van extreem Iers nationalisme geworden.

De regering in Londen zag zichzelf als neutraal. De Ierse nationalisten beschouwden haar echter als partijdig ten gunste van de protestanten. In 1972 kwam er als gevolg van het geweld een eind aan zelfbestuur voor Noord-Ierland. Westminster nam het bestuur direct over.

Ten slotte was ook de regering van de Ierse Republiek in Dublin bij het conflict betrokken. In de grondwet van Ierland was het doel van de politieke vereniging van de graafschappen in Noord-Ierland met de rest van het eiland prominent opgenomen.

Dieptepunten

Ten tijde van de Troubles kenden de gewelddadigheden een paar dieptepunten. Een daarvan was *Bloody Sunday*, op 30 januari 1972. Wat in de stad Derry/Londonderry begon als een vreedzaam katholiek protest tegen de detentie van activisten zonder vorm van proces, werd een veldslag waarbij Britse militairen het vuur openden op de demonstranten. Dertien demonstranten kwamen daarbij om. In het jaar van *Bloody Sunday* kwamen 467 mensen, van wie 321 burgers, om in het geweld.

Een ander dieptepunt vormde de hongerstaking van zeven nationalistische gevangenen in de Maze-gevangenis in Belfast. Zij wilden als politieke gevangenen een andere behandeling dan gewone misdadigers. De Britse minister-president Margaret Thatcher weigerde toe te geven. Dat leidde tot de dood van de hongerstakers, onder wie Bobby Sands, die een martelaar zou worden in de politieke strijd van de IRA.

Een beruchte IRA-aanslag was de moord in augustus 1979 op Lord Louis Mountbatten, een neef van koningin Elizabeth en de laatste Viceroy of India, terwijl hij voor de Ierse kust op zijn jacht voer.

Ten slotte kan de aanslag worden genoemd die de IRA in oktober 1984 pleegde op een hotel in Brighton. Hier vond een vergadering plaats van de Britse Conservatieve Partij. Vijf mensen kwamen om en 34 mensen raken zwaar ge-

wond. Margaret Thatcher ontkwam daarbij ternauwernood aan de dood.

Toenaderingspogingen

Pas in de jaren negentig kwam er langzaam een toenaderingsproces op gang van de verschillende relevante politieke partijen in Noord-Ierland, de regering van Groot-Brittannië en de regering van Ierland. Dit resulteerde in 1998 in het zogeheten *Good Friday Agreement* (Goede Vrijdag-akkoord).¹² Kern van die overeenkomst is dat Noord-Ierland deel blijft uitmaken van het VK tot een meerderheid van de kiezers anders beslist.

Er werd zowel in Noord-Ierland als in de Ierse Republiek een referendum over het Akkoord gehouden. Bij de volksraadpleging in Noord-Ierland (met een opkomst van 81 procent van de kiezers) stemde 71 procent voor en 29 procent tegen. Bij het referendum in Ierland was de opkomst 56 procent. 94 Procent van de opgekomen kiezers stemde voor, 6 procent tegen.

Het Akkoord is enerzijds een overeenkomst tussen acht politieke partijen in Noord-Ierland en anderzijds een internationaal verdrag tussen het VK en Ierland. De regeringen van deze staten erkenden dat de oplossing een zaak was van de bevolking van het hele eiland, zonder inmenging van London.

Noord-Ierland kreeg weer een eigen regering en een eigen parlement. Voor de Ierse Republiek hield de overeenkomst in dat de grondwet werd gewijzigd. Het oude artikel 2 van de grondwet, waarin de Ierse natie aanspraak maakte op soevereiniteit over het hele eiland, werd vervangen door een tekst waarin gesproken werd over referenda in Noord-Ierland en de Ierse Republiek.

Over de instellingen van Noord-Ierland werd vastgelegd dat de regering zetelt in Belfast en wordt samengesteld op basis van power-sharing. Het parlement, de *Northern Ireland Assembly* telt 108 leden en is bevoegd op gebieden die worden aangeduid als *devolved matters* (aangelegenheden betreffende Noord-Ierland).

¹² <http://cain.ulst.ac.uk/events/peace/docs/agreement.pdf>.

De regering en het parlement van het VK is bevoegd op het gebied van *reserved matters* (aangelegenheden betreffende het gehele VK). Er is een *Northern Ireland Office* (NIO), dat de regering van het VK vertegenwoordigt in Noord-Ierland als het gaat om reserved matters. Het behartigt voorts de belangen van Noord-Ierland binnen de regering van het VK. Het NIO staat onder leiding van een minister, die deel uitmaakt van het Britse kabinet.

Bepalingen van het Akkoord

Het Akkoord bepaalt dat er in Noord-Ierland drie politiek relevante gemeenschappen zijn: *nationalist*, *unionist*, en *other*. Elk lid van het parlement geeft aan tot welke gemeenschap hij of zij wil behoren. Beslissingen die de drie groepen overstijgen kunnen alleen met een 'speciale meerderheid' worden genomen.

Key decisions zijn onder meer de verkiezing van de voorzitter van de Assembly, de First Minister en de Deputy First Minister en budgettoewijzingen. Op die manier worden de gemeenschappen beschermd tegen de getalsmatige meerderheid. Ten minste 30 van de 108 leden kunnen vragen om een beslissing te categoriseren als *key decision*. De toewijzing van ministersposten en de samenstelling van de Vaste Commissies vindt plaats op basis van evenredige vertegenwoordiging van de samenstelling van de Assembly. Verkiezingen worden georganiseerd op basis van een districtenstelsel waarin elementen van evenredige vertegenwoordiging verwerkt zijn.

Implementatie van het akkoord

De implementatie van het Goede Vrijdag-akkoord ging moeizaam. Er was tijd nodig voor de uitvoering van bepalingen als de ontwapening van de Provisional IRA, de demobilisatie van paramilitairen en politiehervorming. Pas op 28 juli 2005 verklaarde de IRA dat haar 'militaire' campagne was beëindigd en begon ze met de ontmanteling van haar wapenarsenaal.

Na de verkiezingen in maart 2007 kreeg Noord-Ierland een eigen regering onder leiding van dominee Ian Paisley (DUP) als First Minister en Martin McGuinness (Sinn Fein) als Deputy First

Minister. Inmiddels heeft Peter Robinson (DUP) Ian Paisley opgevolgd als minister-president. Op grond van de regels van machtsdeling bestaat de Executive sinds 2011 uit 4 posten voor de DUP, 3 voor Sinn Fein, 1 voor de SDLP, 1 voor de UUP en 1 voor de Alliance partij.

Uitslagen verkiezingen Northern Ireland Assembly

Partij	zetels maart 2007	zetels mei 2011
Unionist		
DUP	36	38
UUP	18	16
Progressive Unionist	1	-
Traditional Unionist	-	1
Totaal Unionist	55	55
Nationalist		
Sinn Fein	28	29
SDLP	16	14
Totaal Nationalist	44	43
"Other"		
Alliance	7	8
Independent	1	1
Green	1	1
Totaal Other	9	10
Totaal	108	108

De theorie van machtsdeling

Het hiervoor beschreven Goede Vrijdag-akkoord kan worden beschouwd als een experiment met theorieën over machtsdeling die onder meer zijn voortgekomen uit het gedachtegoed van de Nederlandse politicoloog Arend Lijphart.

Power-sharing is een concept dat een goed functionerende democratie in sterk verdeelde samenlevingen mogelijk wil maken. Lijphart heeft het ontwikkeld op basis van studies over Nederland, België en Zwitserland. Later zijn daar onderzoeken naar complexe samenlevingen



FOTO AUTEUR

Een muurschildering in de protestantse Shankill Road wijk, in Belfast, die de Ulster Volunteer Force (UVF; een protestantse vigilante groep) verheerlijkt. Vermoedelijk zijn personen uit de UVF betrokken bij de recente rellen

– zoals Libanon en Zuid-Afrika – bijgekomen. Power-sharing is geëvolueerd van een theorie die bestaande democratische stelsels verklaart naar een theorie met een normatief karakter. In dat opzicht is de theorie ook relevant voor post-conflict stabilisatiemissies elders in de wereld.

Een democratie op basis van power-sharing onderscheidt zich van een democratie op basis van regeren per meerderheid (*majoritarian democracy*). Majoritarian democracy kan leiden tot de permanente politieke uitsluiting van bijna de helft van de bevolking, aangezien een parlementaire meerderheid van net iets meer dan vijftig procent van de stemmen voldoende is om de macht uit te oefenen. Dat geldt vooral in

landen waarin een taalkundige, culturele of religieuze minderheid woont. Zeker in situaties waarin dergelijke kenmerken politiek relevant zijn, zal zo'n minderheid nooit in staat zijn om in de toekomst de politieke meerderheid uit te maken.

Twee benaderingen

Voor wie dat niet wil, zijn er grofweg twee manieren om met een verdeelde samenleving om te gaan. De ene benadering beoogt mobilisering van kiezers op grond van nationale, etnische, religieuze of culturele eigenschappen te ontmoedigen en integratie in overkoepelende politieke partijen te bevorderen. In die visie zijn identiteiten niet statisch, maar dynamisch.

Aan de andere kant staan de voorstanders van power-sharing.¹³ Deze groep wil politieke rechten aan minderheden toekennen en hen in staat stellen een reële invloed uit te oefenen op het overheidsbeleid. Dat zou onder meer moeten gebeuren door een uitvoerende macht waarin alle relevante minderheden zijn vertegenwoordigd, een meerpartijendemocratie met evenredige vertegenwoordiging en de mogelijkheid voor minderheden om kwesties die voor de eigen groep belangrijk zijn, zelf te regelen.¹⁴

Het is een soort federalisme, waarin politieke bevoegdheden niet op regionale worden toegekend, maar op etnische of culturele basis.

Het Goede Vrijdag-akkoord is gebaseerd op het model van Lijphart. Sterker nog, volgens Rupert Taylor: '(...) Northern Ireland has ostensibly become the key confirming case for consociational theory (...)'¹⁵ Ook volgens Donald Horowitz is de overeenkomst 'strongly consociational'.¹⁶ In de uitvoerende macht zijn namelijk alle gemeenschappen op basis van evenredigheid vertegenwoordigd. Evenredigheid wordt ook toegepast in het kiessysteem. En er zijn garanties voor de bescherming van die aangelegenheden die voor de minderheden van bijzonder belang zijn.

Nadelen van machtsdeling

Aan power-sharing worden ook nadelen toegeschreven. Een daarvan is de neiging om verschil-

13 John McGarry and Brendan O'Leary, 'Power Shared after the Death of Thousands', Rupert Taylor (Ed.) *Consociational Theory; McGarry and O'Leary and the Northern Ireland Conflict* (London / New York: Routledge 2009) 16-17.

14 Zie: Arend Lijphart, *Patterns of democracy: Government Forms and Performance in Thirty-Six Countries* (New Haven / London: Yale University Press 1999).

15 Rupert Taylor, 'Introduction', Rupert Taylor (Ed.) *Consociational Theory; McGarry and O'Leary and the Northern Ireland Conflict* (London / New York: Routledge 2009) 10.

16 Donald L. Horowitz, 'Explaining the Northern Ireland Agreement: The Sources of an Unlikely Consensus', *British Journal of Political Science* (Volume 32/Issue 02, March 2002) 194.

len vast te leggen in plaats van te verzachten. Daar is ook in Noord-Ierland sprake van. Ten eerste omdat de politieke boventoon gevoerd wordt door de meest radicale partijen van de beide gemeenschappen: Sinn Fein en de DUP.

De onderhandelingen werden vooral gevoerd tussen de SDLP en de UUP. Pas na de nodige aanpassingen waren ook Sinn Fein en de DUP bereid om voluit in het nieuwe systeem mee te draaien. Zij hadden de meeste afstand bewaard ten opzichte van de onderhandelingen en zich mede daardoor kunnen profileren als de meest authentieke vertegenwoordigers van hun gemeenschap. De meeste kiezers waren akkoord gegaan met de nieuwe constitutionele bedeling, maar daarbinnen gaven zij de voorkeur aan de meest radicale stem van hun identiteit.¹⁷

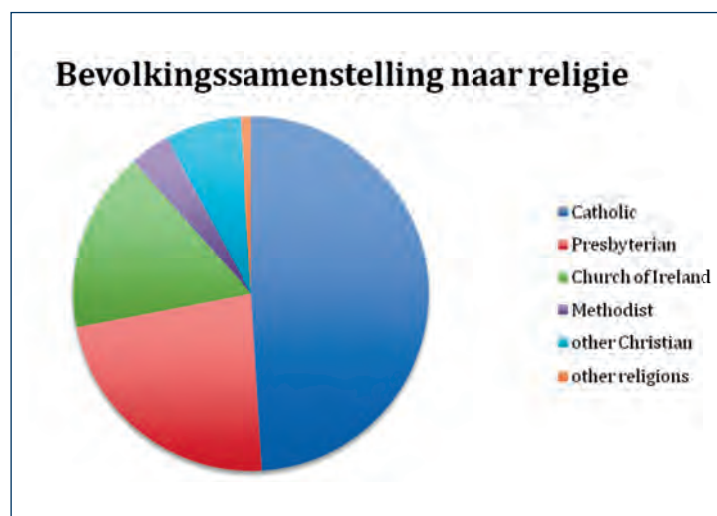
Ten tweede omdat de nationalistische en unionistische identiteit niet alleen politiek maar ook maatschappelijk nog steeds het belangrijkste kenmerk is van de gemeenschappen waar de inwoners toe behoren, aldus Farry.¹⁸ En ten derde bestaat er nog steeds geen overkoepelende politieke identiteit die burgers van Noord-Ierland samenbindt.

Ook het Goede Vrijdag-akkoord laat de politieke toekomst open. Dat kan ook niet anders, omdat de gemeenschappen hierover fundamenteel van mening verschillen. De nationalist willen aansluiting bij Ierland; de unionisten willen aangesloten blijven bij het VK. En er zijn inwoners die graag een sterkere afzonderlijke Noord-Ierse identiteit zouden zien. Er wordt dan ook geen beleid gevoerd dat een gemeenschappelijke visie op de toekomst bevordert.

Tot op de dag van vandaag blijft Noord-Ierland sterk verdeeld. Uit een groot bevolkingsonderzoek, waarvan de resultaten in december 2012 werden gepubliceerd, bleek het volgende. Van de 1,8 miljoen inwoners van Noord-Ierland zegt 41 procent katholiek te zijn, 19 procent presbyteriaans, 14 procent anglicaans, 3 procent methodist, 6 procent hangt een andere christelijke religie aan, 1 procent zegt een niet-christelijke religie te belijden, 10 procent geeft op 'geen religie' en 7 procent vult niets in.¹⁹

Op de vraag tot welke nationale identiteit de ondervraagden zich rekenden kwamen de volgende gegevens naar voren: 40 procent van de inwoners van Noord-Ierland gaf aan een 'British Only' identiteit te hebben, 25 procent voelde zich 'Irish Only' en 21 procent 'Northern Irish Only'. Bij de beantwoording van deze vraag was het niet mogelijk meer dan één nationale identiteit in te vullen.

Wanneer er wel meerdere antwoorden mogelijk waren, noemde 48 procent van de bevolking zich British, 29 procent Northern Irish, 28 procent Irish en gaf 5 procent een andere identiteit aan.²⁰ Daaruit kan worden afgeleid dat er onder de Noord-Ierse bevolking nog steeds een sterke verdeeldheid is over de nationale identiteit.



Figuur 1: Bevolkingsamenstelling naar religie.

Bron: Census 2011; Key Statistics for Northern Ireland, Northern Ireland Statistics and Research Agency (Belfast December 2012) 19, http://www.nisra.gov.uk/Census/key_stats_bulletin_2011.pdf

17 Zie noot 13, 57.

18 Stephen Farry, 'Consociationalism and the Creation of a Shared Future for Northern Ireland' Rupert Taylor (Ed.) *Consociational Theory*; McGarry and O'Leary and the Northern Ireland Conflict (London / New York: Routledge 2009) 170.

19 Census 2011; Key Statistics for Northern Ireland, Northern Ireland Statistics and Research Agency (Belfast December 2012) 19.

20 Census 2011; Key Statistics for Northern Ireland, 12-13.

Oorzaken van de recente rellen

De lange voorgeschiedenis van achterstelling, geweld en de politieke consolidatie van culturele verschillen vormen de achtergrond waartegen de recente rellen moeten worden bekeken.²¹ Op het eerste gezicht gaat de *Belfast Flag Issue* over het voeren van een vlag die voor unionisten dierbaar is. Maar dieper daaronder ligt de vrees van de relschoppers dat zij door Groot-Britannië in de steek gelaten zijn.

Dit vormt de eerste oorzaak van de rellen. Tot aan het Goede Vrijdag-akkoord hadden de unionisten in Noord-Ierland duidelijk meer politieke, economische en maatschappelijke macht. Na decennia van dominantie hebben zij het niet meer alleen voor het zeggen. Nu beschouwen ze zichzelf als de verliezers van het vredesproces.

Het waren trouwens de unionisten die in de vredesonderhandelingen het meeste afstand hielden. Ook toen het referendum over het Goede Vrijdag-akkoord in Noord-Ierland werd gehouden, was de steun onder de protestanten het laagst. De reden waarom de meer gematigde unionistische partij, de UUP, kon instemmen met het Goede Vrijdag-akkoord ligt volgens Horowitz vooral in de vrees onder unionisten dat ze vanwege demografische ontwikkelingen in de toekomst zelf wel eens een minderheid in Noord-Ierland zouden kunnen vormen. Zij zouden dus vooral om defensieve redenen hebben ingestemd met het Akkoord.²²

Nieuwe 'tweederangsburgers'

Door de power-sharing arrangementen en evenredigheid als verdeelsleutel kregen de katholieken steeds meer invloed in Noord-Ierland. Bovendien waren zij er vanuit hun achterstandssituatie al lang van doordrongen dat ze alleen door goed leren en hard werken hun situatie konden verbeteren. Ze werden hierdoor beter gekwalificeerd voor de arbeidsmarkt dan de protestanten.²³

De rollen lijken daarmee omgedraaid.²⁴ Protestantse jongeren voelen zich nu, zoals een van hen in een interview voor de Duitse televisie vertelde, tweederangsburgers.²⁵ Nog verder gaat de afkeer die de orthodox-protestantse achterban van de DUP begint te krijgen ten opzichte van Groot-Britannië, dat zij als goddeloos ervaren. Zij trekken zich steeds verder uit het publieke leven terug en zoeken hun heil in het geloof en in de troost dat het aardse leven maar een tussenstation is op weg naar verlossing.²⁶

Deze laatste categorie vormt echter alleen niet de relschoppers. Volgens Gareth Mulvenna, verbonden aan de Queen's University Belfast, zijn dat veeleer protestantse jongeren uit de arbeidersklasse, die in de economisch achtergestelde wijken van Belfast (Shankill, Tiger's Bay en Dee Street) wonen.²⁷

Mulvenna laat zien dat deze jongeren zich in een nadelige situatie bevinden vanwege een lage opleiding en een grote kans op werkeloosheid. En ten slotte merkt hij op dat grote groepen sinds 1971 uit de slechte wijken zijn weggetrokken en dat mede hierdoor het religieuze en maatschappelijke engagement en het opleidingsniveau van veel protestanten uit de arbeidersklasse sterk is afgenomen.²⁸

Verdwijnen van burgerzin

In de jaren van de Troubles zijn traditionele verbanden, vooral die van kerk en sportclub, uit elkaar gevallen. Protestantse jongeren begonnen zich te organiseren in zogeheten Tartan-gangs. Die boden hen een uitlaatklep voor hun frustraties.²⁹ Tevens kwamen de jongeren steeds meer in aanraking met paramilitairen,

21 De inschattingen van deze paragraaf zijn mede gebaseerd op persoonlijke gesprekken met experts in Noord-Ierland en Ierland.

22 Donald L. Horowitz, 'Explaining the Northern Ireland Agreement: The Sources of an Unlikely Consensus', *British Journal of Political Science* (Volume 32/Issue 02, March 2002) 201-202.

23 'Veel loyalisten voelen zich bedreigd in hun Britsheid', NRC Handelsblad, 10 januari 2013.

24 David McKittrick and David McVea, *Making Sense of the Troubles: a History of the Northern Ireland Conflict* (London: Viking/Penguin Group 2012) 290-293.

25 www.tagesschau.de/ausland/unruhen-belfast104.html.

26 Claire Mitchell and Jennifer Todd, *Between the Devil and the Deep Blue Sea: Nationality, Power and Symbolic Trade-offs among Evangelical Protestants in Contemporary Northern Ireland*, *Nations and Nationalism* (Volume 13 No. 4, 2007) 637-655.

27 www.guardian.co.uk/commentisfree/2012/dec/05/belfast-union-flag-loyalists.

28 Gareth Mulvenna, 'The Protestant Working Class in Belfast: Education and Civic Erosion – an Alternative Analysis', *Irish Studies Review* (Volume 20, No. 4, November 2012) 439-441.

29 Zie noot 28, 438.

zoals de UVF, die deze bendes gebruikten om nieuwe leden te rekruteren.³⁰ Met andere woorden, de burgerzin, die voordien deel uitmaakte van de protestantse ethos, begon langzaam aan te verdwijnen.

Geen verzoening

De tweede oorzaak van de onlusten moet worden gezocht in de wijze waarop het vredesproces vorm heeft gekregen. De vredesovereenkomst van 1998 werd uitgewerkt in vooral statelijke – regionale en lokale – instituties. De vrede was een *top-down* proces.

Verzoening van onderop is tot nu toe beperkt gebleven. De protestantse en katholieke bevolkingsgroepen leven nog steeds sterk geïsoleerd ten opzichte van elkaar, hetgeen gesymboliseerd wordt door de metershoge scheidingsmuren langs de *interfaces*, de grenzen tussen de katholieke en protestantse wijken.

Blijkens de volksraadpleging van 2011 beschouwde 21 procent van de bevolking de eigen identiteit ondertussen als exclusief Noord-Iers (zie terug). Dat lijkt een nieuwe ontwikkeling te zijn, al is het ontstaan van een gemeenschappelijke Noord-Ierse *civil society* nog ver verwijderd.

De slechte economische omstandigheden zijn ongetwijfeld een derde oorzaak van de rellen. Ondanks een jaarlijkse subsidie voor Noord-Ierland van acht miljard pond stijgt de werkloosheid en zijn de toekomstperspectieven voor veel jongeren ongewis. Het gevoel van onzekerheid en het gevoel door Londen in de steek te zijn gelaten, lijkt sinds de Goede Vrijdag-akkoorden te zijn toegenomen.³¹ Volgens een volkstelling (census) uit 2011 ligt de jeugdwerkloosheid (16-24 jarigen) rond de 29 procent.³² Al deze factoren hebben bijgedragen aan de jongste rellen in Belfast.

Sociale media

Het is opvallend dat de rol van de sociale media in het publieke debat tot nu toe nauwelijks is belicht. Gezien de samenstelling van de demonstranten zou het ons niet verbazen als nieuwe communicatiemiddelen – waaronder sms

bombs, crowd gathering via sms alerts, Facebook en Twitter – een belangrijk organisatie-medium zijn.

De BBC vermoedt dat de nieuwe sociale media bij de organisatie van de acties worden gebruikt.³³ Dit artikel tracht de recente rellen te verklaren en in een politieke context te plaatsen. Onderzoek naar de rol van sociale media is zinvol, maar valt buiten het bestek van deze bijdrage.

Riskante perspectieven

Niet alleen de huidige onrust wordt sterk bepaald door symboliek. Ook in de komende jaren zijn er gebeurtenissen te verwachten met een sterk symbolische betekenis, die ongetwijfeld effecten zullen hebben op het vredesproces. In chronologische volgorde zijn dat: de discussie over het Britse lidmaatschap van de Europese Unie, het referendum in 2014 over de onafhankelijkheid van Schotland, en de herdenking van de Paasopstand in Dublin in 1916.

Discussie over Brits EU-lidmaatschap

De Britse premier David Cameron hield op 23 januari 2013 in Londen een toespraak over de toekomst van het Britse lidmaatschap van de Europese Unie. Hij nam daarin afstand van het streven naar een steeds hechtere unie van de volken van Europa, zoals verwoord in het Europese Verdrag.

Er moet juist meer macht terug naar de lidstaten, vindt Cameron: *'Countries in Europe have their histories, their traditions, their institutions, want their own sovereignty, their ability to make their own choices, and to try and shoehorn countries into a centralised political union would be a great mistake for Europe, and Britain wouldn't be part of it'*.

30 Gareth Mulvenna, *The Protestant Working Class*, 438.

31 Gesprek van de auteurs met experts op Queen's University Belfast (07-01-2013) en National University of Ireland in Maynooth (09-01-2013).

32 *Census 2011; Key Statistics for Northern Ireland*, 28.

33 www.bbc.co.uk/news/uk-northern-ireland-20651163. Het onderwerp sociale media als vorm van organisatie van protesten verdient nader onderzoek, temeer omdat sociale media ook een rol speelden bij de recente rellen in Haren (Gr) en vermoedelijk ook een bepaalde dynamiek aan de zogeheten Arabische Lente hebben gegeven.



FOTO REUTERS

Premier David Cameron nam onlangs tijdens een toespraak in Londen afstand van het streven naar een hechtere Europese Unie

Cameron beloofde dat hij zal onderhandelen over een nieuw verdrag wanneer hij bij de volgende Britse parlementsverkiezingen wordt herkozen. Daarna zal hij een referendum organiseren over de vraag of het VK lid moet blijven van de EU.³⁴

Als dat referendum een Brits 'nee' tegen de Europese Unie zou opleveren, zou dat verstrekende gevolgen hebben voor de relatie met de Ierse Republiek en de positie van Noord-Ierland. Juist de open grens tussen Noord-Ierland en de Republiek en het lidmaatschap van Ierland en Groot-Brittannië van de EU hebben de gevolgen van de Ierse deling in noord en zuid verzacht. De EU is daarnaast een leverancier van omvangrijke subsidies ten gunste van verzoening en economische ontwikkeling. Dat zou allemaal ter discussie worden gesteld. Enda Kenny, premier van Ierland (*taoiseach*), heeft al gereageerd met de opmerking dat hij geen manier zag waarop het EU-verdrag opnieuw voorwerp zou

worden van onderhandeling, tenzij met het oog op hechtere integratie.³⁵

Schots referendum in 2014

In 2014 vindt in Schotland een volksraadpleging plaats over de vraag of Schotland onafhankelijk moet worden. Als Schotland het VK verlaat zal het VK bestaan uit een groot en dominant Engeland en de twee kleine, perifere delen Wales en Noord-Ierland.

De protestanten in Noord-Ierland hebben altijd een nauwe verbondenheid gevoeld met protestanten in Schotland. Bij een Schotse afscheiding zullen zij zich nog meer verweesd voelen in het VK.³⁶ Het is dan ook niet verwonderlijk dat Peter Robinson, First Minister van Noord-Ierland en leider van de DUP, in januari 2012 tijdens een bijeenkomst in Dublin grote zorgen over een Schotse onafhankelijkheid uitte: *'Our peoples have moved from one side of that small stretch of water to the other and back again many times over the centuries. So we have a massive interest and I don't think we can sit idly by and simply indicate that it is a matter for Scotland alone. It will have implications for us all. We hope that Scotland knows just how much we want them to remain within the UK.'*³⁷

Aan de andere kant zullen de republikeinen een mogelijke Schotse afscheiding met grote belangstelling volgen. Succes voor de Schotse nationalisten kan een aanmoediging zijn voor Sinn Féin *'to capitalise on the new, more fluid approach towards the UK's constitutional arrangements by putting the issue of Irish unity firmly on the political agenda (...) That's the driving logic'*.³⁸

Volgens columnist Alex Salmond zullen republikeinen in Noord-Ierland met interesse toezien hoe de Britse aanwezigheid in Schotland ten einde zal komen. Vlaggen die worden gestreken, militairen die zich terugtrekken, anti-Engelse gevoelens die de boventoon zullen voeren, maar ook interne tegenstellingen die zich van Noord-Ierland naar Schotland zullen verspreiden.³⁹

Herdenking Paasopstand

Dan wordt ten slotte in 2016 herdacht dat Ierse nationalisten in 1916 in Dublin in opstand

34 www.number10.gov.uk/news/eu-speech-at-bloomberg.

35 <http://uk.reuters.com/article/2013/01/24/uk-davos-cameron-europe-idUKBRE90NOCY20130124>.

36 Mary Kenny, 'Scottish "Divorce" will throw North's Identity into Chaos', *Independent*, January 16 2012, www.independent.ie.

37 Nicholas Watt, 'Scottish Independence: Wales and Northern Ireland make Unity Plea', *The Guardian*, 13 January 2012, www.guardian.co.uk/politics/2012/jan/13/scottish-independence-wales-northern-ireland.

38 James Maxwell, 'Scottish Independence: The View from Belfast', *The New Statesman*, 2 July 2012, www.newstatesman.com.

39 'The Northern Irish Question; Alex Salmond's Ticking Bomb', *The Week*, 20 January 2012, www.theweek.co.uk.

kwamen en de onafhankelijkheid van Ierland uitriepen: de *Easter Rising*. De opstand werd in een paar dagen door de Britten onderdrukt. In dat verband heeft Sinn Fein-leider Martin McGuinness nog maar weer eens verklaard dat hij in 2016 een referendum wil over de vraag of er een verenigd Ierland moet komen.

In een reactie zei Peter Weir, *chief whip* van de DUP, dat hij erop vertrouwt dat Noord-Ierland in 2021 zijn honderdjarig bestaan als staat zal vieren en ambitieuze plannen zal ontwikkelen voor de volgende honderd jaar.⁴⁰

Conclusies

Het conflict in Noord-Ierland leek vergeten. Sinds de Goede Vrijdag-akkoorden in 1998 was het relatief rustig. De westerse wereld concen-

treerde zich op andere conflicten. Het vredesproces in Noord-Ierland blijkt echter van verschillende kanten onder druk te staan. Deels wordt deze druk veroorzaakt door uiteenlopende verwachtingen over politieke ontwikkelingen in de toekomst. De discussie over het Britse lidmaatschap van de EU, de mogelijkheid dat Schotland zich losmaakt uit het VK of de verwachtingen die worden opgeroepen door een historische datum vormen risicofactoren voor het verdere verloop van het vredesproces.

Daarnaast hebben vooral de recente gebeurtenissen in Noord-Ierland, en dan vooral de vlaggenkwesie, duidelijk gemaakt hoe kwetsbaar

40 'McGuinness wants referendum on united Ireland by 2016', The Irish News, 31 January 2012, www.irishnews.com/news/story/1128631.



De metershoge scheidingsmuur tussen de beide katholieke en protestantse wijken. Ook het Goede Vrijdag-akkoord laat de politieke toekomst open. Dat kan ook niet anders, omdat de gemeenschappen hierover fundamenteel van mening verschillen

FOTO AUTEUR

de vrede nu nog steeds is. Het gekozen constitutionele model leek een rechtvaardige oplossing te bieden voor de omgang met nationale minderheden. Tegelijk werd met het beginsel van machtsdeling de verdeeldheid van de samenleving geïnstitutionaliseerd.

Tevens speelt onder unionisten het gevoel een rol dat Noord-Ierland maar een perifeer gebied is, dat nauwelijks de aandacht van het politieke centrum heeft. Deze gevoelens worden door de gevolgen van de financieel-economische crisis versterkt en worden door onruststokers uitgebuit.

Als het goed gaat in Noord-Ierland raakt dat ook Nederland.

Als er risico's zijn, zoals met de recente rellen, moet ook Den Haag alert zijn

Wij hebben getracht de oorzaken van de recente protesten en rellen in kaart te brengen. Er zijn verschillende factoren naar voren gekomen, die aan de basis liggen van een steeds toenemende ontevredenheid bij vooral de protestantse arbeidersklasse: religie, nationalisme en sociaaleconomische omstandigheden. Recente onderzoeken die in dit artikel zijn verwerkt, duiden erop dat de vrede niet alleen winnaars heeft. Er is ook een belangrijke groep, in het bijzonder de protestantse arbeidersklasse, die in objectieve zin wellicht geen verliezer is, maar die zich desalniettemin wel zo voelt.

Het is de moeite waard om deze vraagstukken in Noord-Ierland aan een nadere beschouwing te onderwerpen. Het conflict en het vredesproces vertonen parallellen met andere recente conflicten in de wereld. Conflicten, waarbij ook Nederland heeft getracht aan de oplossing bij te dragen. Nederland heeft er niet alleen belang

bij dat er in buurland VK vrede heerst, maar ook in de landen waar het zelf de laatste twintig jaar heeft ingegrepen. Als het goed gaat in Noord-Ierland raakt dat ook Nederland. Als er risico's zijn, zoals met de recente rellen, moet ook Den Haag alert zijn.

Natuurlijk is wat in Belfast gebeurt niet één op één toepasbaar op Sarajevo of Kabul. Maar het is wel degelijk mogelijk om lessen te trekken uit het vredesproces in Noord-Ierland. Niet alleen voor militaire strategieën en tactieken, zoals counterinsurgency en policing, maar vooral voor een echte comprehensive approach, waar alle bij de conflictbeslechting betrokken partijen langdurig bij betrokken moeten blijven.

De eerste conclusie die zich aandient is natuurlijk de constatering dat vredesprocessen een lange tijd nodig hebben. Maar daarna rijst onherroepelijk de vraag hoe Nederland, Europa en de Verenigde Naties kunnen bijdragen aan een duurzame vrede op de Balkan, de Hindukush of Noord- en Centraal-Afrika als het niet eens mogelijk is een duurzame vrede op te bouwen in een gebied waarvan de hoofdstad, Belfast, geen twee uur vliegen van Den Haag vandaan ligt? Met dit artikel hopen wij ook het debat voor toekomstige missies van Nederland weer te voeden. ■

Onderzoek naar Allied Force staft toekenning vaandelopschrift Koninklijke Luchtmacht

De Commandant Luchtstrijdkrachten stelde de minister van Defensie in 2010 voor om de luchtmacht in aanmerking te laten komen voor een vaandelopschrift voor de Kosovo-campagne in 1999 (operatie *Allied Force*). Overeenkomstig de procedure voor het verkrijgen van een vaandel- of standaardopschrift vroeg de bewindsman advies van de Traditiecommissie Krijgsmacht en het Nederlands Instituut voor Militaire Historie. De bevindingen van een verificatieonderzoek naar het optreden van de KLu in de Kosovo-oorlog waren positief en bij Koninklijk Besluit is op voordracht van de minister besloten tot een aanvulling van het vaandel van de luchtmacht. Op 27 maart 2013 zal Hare Majesteit de Koningin een cravate (vaandeldecoratie) met daarop 'Kosovo 1999' op het vaandel aanbrengen. Welke acties van de KLu tijdens Allied Force hebben tot deze uitzonderlijke collectieve onderscheiding geleid en welke toetsingscriteria zijn er gehanteerd?

Drs. J. Müller en drs. R. de Winter*

De junidagen van 1999 zouden beslissend zijn voor de goede afloop van de NAVO-luchtoperatie *Allied Force*, die president Milosevic op de knieën moest zien te brengen. Al ruim drie maanden vielen NAVO-vliegtuigen doelen aan in voormalig Joegoslavië. Wanneer zou Milosevic opgeven en zich terugtrekken uit Kosovo? Begin juni wist de Servische leider nog van geen wijken. Dat merkten ook twee F-16-vliegers van de Koninklijke Luchtmacht in de nacht van 7 op 8 juni. Zij hadden als missie om een luchtmachtbasis in de buurt van Belgrado aan te vallen. Eenmaal boven de basis ontdekte kapitein-vlieger Marcel Duivesteijn, de leider van de aanval, dat er MiG-29's aanwezig waren.

De dreiging van grond-lucht-raketten bleek bovendien zeer reëel en twee werden er dan ook afgevuurd op het toestel van Duivesteijn. De eerste raket wist hij te ontwijken door zijn vliegtuig ijlings van links naar rechts en van boven naar beneden te verplaatsen.¹ De tweede raket was hardnekkiger: 'Ik zag echter dat het niet ging lukken en dat ik deze tweede SA-3 niet op dezelfde manier kon bedotten. Bovendien bevond hij zich al veel te dichtbij. Ik kon daarop alleen nog maar het allerlaatste redmiddel proberen om hem te ontwijken, een *last ditch*-manoeuvre. Ik maakte een *barrel roll*, een rollende manoeuvre om de missile heen, waarop de raket rakelings langs me heen schoot'.² Duivesteijn schatte dat de raket hem op enkele meters miste.³ Het gevaar was nog niet geweken. In zijn rollende manoeuvre raakte hij verblind door het felle schijnsel van de raketmotor. Op dat moment hing hij ondersteboven en koerste richting aarde: 'Ik kon zowel boven als onder me lichtjes onder-

* Jaus Müller is publicist. Rolf de Winter is senior wetenschappelijk medewerker bij het Nederlands Instituut voor Militaire Historie.

1 Erwin van Loo, *Crossing the border. De Koninklijke Luchtmacht na de val van de Berlijnse Muur* (Den Haag, Sdu Uitgevers, 2003) 708.

2 Idem, 708.

3 Idem, 708.

scheiden, alleen kon ik niet zien wat sterren waren en wat verlichting op de grond was'.⁴ Pas toen hij boven zich de bewegende flitsen van lichtspoorruitie zag, besepte de vlieger dat hij nog altijd op z'n kop vloog. Toen zat hij op 3.300 voet, oftewel slechts één kilometer boven de grond. Zijn *wingman* probeerde intussen de dreiging vanaf de grond weg te nemen door de aandacht op zichzelf te vestigen. Zijn toestel stootte een groot aantal *flares* uit. In reactie hierop werd de *wingman* door luchtafweergeschut onder vuur genomen. Kapitein-vlieger Duivesteijn had intussen meer tijd om naar een veiligere hoogte te klimmen. De MiG's werden alsnog vernietigd en voor deze actie ontvingen kapitein-vlieger Duivesteijn en zijn *wingman*, de Amerikaanse uitwisselingsvlieger majoor W.L. Thomas, het *Vliegerkruis*. Het was voor het eerst in vijftig jaar dat deze dapperheidsonderscheiding werd uitgereikt.

Collectieve onderscheiding?

Bovenstaand voorbeeld toont aan met wat voor moed en beleid de vliegers te werk gingen. Maar zijn dit soort individuele heldendaden voldoende om de luchtmacht als collectief te onderscheiden? Die vraag kwam in 2010 aan de orde toen de Commandant Luchtstrijdkrachten de minister van Defensie voorstelde om de luchtmacht in aanmerking te laten komen voor een vaandelopschrift voor de Kosovo-campagne in 1999. Overeenkomstig de procedure voor het verkrijgen van een vaandel- of standaardopschrift vroeg de bewindsman advies van de Traditiecommissie Krijgsmacht en het Nederlands Instituut voor Militaire Historie (NIMH). Dat resulteerde in een zes maanden durend (verificatie)onderzoek naar het optreden van de luchtmacht in de Kosovo-oorlog. Het eindoordeel luidde positief en bij Koninklijk Besluit van 5 maart 2012 is op voordracht van de minister van Defensie besloten tot aanvulling van het



De toekenning van vaandelopschriften bij de krijgsmacht is uitzonderlijk

vaandel van de luchtmacht. Op 27 maart 2013 zal Hare Majesteit de Koningin een cravate (vaandeldecoratie) met daarop 'Kosovo 1999' op het vaandel aanbrengen.⁵

In dit artikel zal de vraag worden beantwoord op welke gronden de Koninklijke Luchtmacht dit vaandelopschrift krijgt en welke aspecten daarbij zijn meegewogen. Het is de moeite waard om hier wat langer bij stil te staan, want het is uitzonderlijk dat een vaandelopschrift wordt toegekend. Bij de luchtmacht gebeurde dat voor het laatst in 1965. De luchtmacht kreeg dat jaar haar vaandel uitgereikt met daarop de volgende opschriften: Nederland 1940; Nederlands-Indië/Malakka 1941-1942; Engeland/West-Europa 1941-1945 en Australië/Indische Archipel 1942-1945.⁶ Sindsdien kwamen daar voor de luchtmacht op het vaandel geen nieuwe wapenfeiten meer bij.

Aanloop naar de Kosovo-crisis

Allereerst een stap terug in de geschiedenis, naar het eind van de twintigste eeuw. Wat gebeurde er in Kosovo, hoe raakte Nederland betrokken bij de Kosovo-crisis en hoe verliep de uitvoering van de luchtcampagne door de luchtmacht? Eind jaren negentig liepen de spanningen in Kosovo maand na maand verder

4 Idem, 709.

5 Rijksvoorlichtingsdienst, RVD nr. 15, *Koningin brengt decoratie 'Kosovo 1999' aan op vaandel Koninklijke Luchtmacht* (22 januari 2013).

6 Zie: NIMH, *Het vaandel van de Koninklijke Luchtmacht*, www.defensie.nl/nimh/geschiedenis/vaandels_en_standaarden/vaandels_en_standaarden_koninklijke_luchtmacht/vaandel_van_de_koninklijke_luchtmacht.



FOTO KONINKLIJKE LUCHTWACHT

Nederland speelde in het onderhandelingscircuit een ondergeschikte rol.⁷ Pas toen de kwestie na de mislukte onderhandelingen verschoof van de EU naar de NAVO, nam de invloed van Nederland toe. De NAVO verzocht Nederland mee te doen aan een militaire interventie. Drie argumenten gaven voor de Nederlandse politiek de doorslag om deel te nemen aan de NAVO-operatie Allied Force. Ten eerste bracht de Kosovo-crisis de toch al precare veiligheidssituatie op de Balkan verder in gevaar, want de problemen in Kosovo bedreigden het moeizame vredesproces in Bosnië-Herzegovina. Ook was er het gevaar dat etnisch-Albanezen in andere delen van de Balkan, zoals in Albanië en Macedonië, in opstand zouden komen. Ten tweede, zo vond het parlement, moest een humanitaire crisis als gevolg van etnische zuiveringen en grote stromen vluchtelingen een halt toe worden geroepen. En ten derde wilde de NAVO geen gezichtsverlies lijden: het bestand van oktober 1998 stond onder druk – en daarmee ook de geloofwaardigheid van de alliantie.⁸

Een optimistisch begin

Op woensdagavond 24 maart 1999 ging de operatie van start. In de eerste nacht werd gepoogd de luchtverdediging zoveel mogelijk uit te schakelen. SAM-batterijen, communicatiecentra, vliegvelden en radarinstallaties vormden de voornaamste doelwitten.⁹ De start van Allied Force verliep tamelijk rommelig, want militairen moesten wel erg snel tot actie overgaan toen diplomaten met lege handen terugkeerden van de onderhandelingstafel. Een vastomlijnde strategie ontbrak. Over één ding waren de negentien deelnemende NAVO-landen het wél eens: Milosevic moest worden gestopt. Maar de meningen verschilden hoe die landen dat via de militaire weg konden bereiken.¹⁰ Generaal

7 Brief van minister-president W. Kok, de minister van Buitenlandse Zaken J.J. van Aartsen en de minister van Defensie F.H.G. de Grave aan de Tweede Kamer. 22181 De situatie in voormalig Joegoslavië, nr. 310. 22 maart 2000.

8 Van Loo, *Crossing the border*, 663.

9 Idem, 666.

10 Dag Henriksen, 'Inflexible Response: Diplomacy, Airpower and the Kosovo Crisis, 1998–1999' in: *Journal of Strategic Studies*, 31:6 (2008) 855.

op. Na acht jaar vreedzaam verzet stichtten radicale Albanezen in 1997 het Albanese Bevrijdingsleger (UCK). Er vonden daarna aanslagen plaats op Serviërs en Albanezen die aan de Servische kant van het conflict stonden. Groot-schalig was het gewapend verzet van het UCK niet, maar Belgrado zag voldoende redenen over te gaan tot een militaire interventie. Het leger en paramilitairen joegen Albanezen hun huizen uit. Etnische zuiveringen waren schering en inslag. Een kwart van de totale bevolking van twee miljoen mensen sloeg op de vlucht. Duizenden mensen stierven als gevolg van het geweld. Even keerde de rust terug toen er in 1998 een doorbraak werd geforceerd in de onderhandelingen tussen de Kosovaarse delegatie en de Serviërs, maar al snel werd dit akkoord door Milosevic geschonden. De NAVO wilde hierop een vredesmacht het gebied insturen om toe te zien op de naleving van de afspraken. Milosevic dulde echter geen NAVO-troepen op zijn grondgebied en de betrokken partijen raakten in maart 1999 in een diplomatieke patstelling. Intussen hielden de gevechten in Kosovo aan. De Amerikaanse gezant Richard Holbrooke ondernam nog een ultieme poging. Toen hij met lege handen van de onderhandelingstafel terugkwam, leek een gewapend ingrijpen van de NAVO onafwendbaar.

Wesley Clark, die als *Supreme Allied Commander Europe* (SACEUR) aan het hoofd stond van operatie Allied Force, beschreef de openingsfase van de missie in een terugblik nogal rooskleurig: 'We were going to blind the Yugoslav military by taking out their radars and cripple them by destroying their anti-air missile systems. Then we were going to sweep in with the manned aircraft'.¹¹ De woorden van Clark waren zeker voor de eerste dagen van de operatie wel erg optimistisch, want zoals de vliegers van de KLu zouden merken, was de vijandelijke luchtverdediging op veel plekken nog volop in bedrijf.

Ook de luchtmacht van Milosevic bleek aanvankelijk nog vrij actief. Op de eerste avond van Allied Force kregen Nederlandse vliegers daar meteen al mee te maken. In de planning stond het verkennen en bewaken van het luchtruim boven de hoofdstad van Kosovo, Pristina. De avond nam een andere wending toen de vliegers tijdens de missie het bericht ontvingen dat drie MiG-29's waren opgestegen.¹² Kort daarna kreeg F-16-vlieger majoor Peter Tankink een MiG-29 in het vizier en vuurde hij een radargeleide luchtlucht-raket af. Na een vlucht van dertig seconden trof de raket doel. De vlieger van de MiG-29 ontstapte aan de dood door tijdig met zijn schietstoel het vliegtuig te verlaten.¹³ Het was voor het eerst in vijftig jaar dat een Nederlandse gevechtsvlieger een vijandelijk vliegtuig uitschakelde in een lucht-lucht-gevecht. Weldra werd duidelijk dat dit voor de luchtmacht een bijzondere missie zou worden: er kwamen namelijk meer premiers op naam van de KLu. Zo moesten Nederlandse F-16's op 15 mei 1999 een aanval op een olieraffinaderij uitvoeren. De explosie die hierdoor ontstond werd vastgelegd door satellieten en ging de geschiedenis in als de hevigste ont-ploffing gemeten tijdens Allied Force.

F-16's vlogen zowel overdag als 's avonds en 's nachts. In de eerste fase van de operatie

moesten Nederlandse jachtvliegers onder meer vijandelijke toestellen onderscheppen. De Nederlandse F-16's kregen een breed takenpakket toegemeten: tactische fotoverkenningsvluchten, luchtverdedigingsvluchten, escortevluchten en luchtaanvallen op gronddoelen in Servië, *Close Air Support*-missies in Kosovo en nachtelijke *Fighter Bomber Attacks* in Servië. In de tweede fase van de luchtcampagne, die ongeveer vier dagen na de start van de eerste fase inging, verschoof het accent van *Suppression of Enemy Air Defences* (SEAD) naar een breder spectrum van aanvalsdoelen, zoals communicatie-installaties en concentraties van militaire troepen.¹⁴ Dit werd steeds noodzakelijker omdat Milosevic de tijd die de NAVO nodig had om de luchtverdediging uit te schakelen, gebruikte om zijn politiek van etnische zuivering voort te zetten. Vanaf april 1999 werd de focus van de bombardementen gericht op fabrieken, olieraffinaderijen, depots, bruggen, spoorlijnen en zendmasten van radio en televisie. Met deze tactiek poogde de NAVO het openbare leven in Klein-Joegoslavië (op dat moment bestaande uit Servië en Montenegro) te ontwrichten.



FOTO KONINKLIJKE LUCHTMACHT

Minister van Defensie De Grave in 2002 bij het onderscheiden van de vliegers Thomas en Duivesteyn (eerste en tweede van links) en marinier D. Vonk

Overwinning

In mei 1999 ging de campagne de derde maand in en duurde daarmee aanzienlijk langer dan bij de start was beoogd.¹⁵ Bij de NAVO rees de vraag hoelang het bombarderen nog zou moeten doorgaan en of het niet tijd werd om ook grondtroepen te sturen. Vooruitlopend op een

11 Wesley K. Clark, *Waging Modern War. Bosnia, Kosovo, and the Future of Combat* (New York, PublicAffairs, 2002) 193.

12 Van Loo, *Crossing the border*, 678.

13 Idem, 679.

14 Idem, 667.

15 Henriksen, 'Inflexible Response', 839.

grondoorlog-scenario verdubbelde de NAVO de interventiemacht KFOR alvast van 28.000 tot 50.000 militairen.¹⁶ Intussen werden achter de schermen aan het diplomatieke front successen geboekt om Milosevic te bewegen zijn strijd te staken. Op 3 juni 1999 trok hij zijn troepen terug uit Kosovo. Allied Force werd op 20 juni officieel beëindigd, na maar liefst 37.000 *sorties* van NAVO-vliegtuigen.¹⁷ Tijdens de achtenzeventig dagen durende luchtcampagne verloor geen van de deelnemende NAVO-landen een militair als gevolg van directe krijgshandelingen.

Was Allied Force een succes? In de dagen voorafgaand aan de operatie waren er nogal wat sceptici die meenden dat een luchtoorlog geen kans van slagen had zonder hulp van grondtroepen. Een militair-historicus van naam, John Keegan, gaf ruiterslijk toe dat hij er naast zat. Hij vergeleek 3 juni 1999 (de dag waarop Milosevic zijn troepen terugtrok) in militair-historisch opzicht met grote keerpunten in de krijgshistorie zoals 20 november 1917, toen bij Cambrai de inzet van tanks voor het eerst de traditionele dominantie van infanterie en cavalerie doorbrak, of 11 november 1940, toen vliegtuigen in staat bleken de eens zo machtige oorlogsbodems te vernietigen tijdens een aanval op de Italiaanse vloot bij Taranto. *'Now there is a new turning point to fix the calendar: June 3, 1999, when the capitulation of President Milosevic proved that a war can be won by airpower alone'*, zei Keegan.¹⁸ Volgens sommigen, onder wie ook Keegan, was het NAVO-luchtoffensief een uniek bewijs dat airpower het gedrag van de tegenstander kan beïnvloeden. Diplomatie en de dreiging van grondtroepen speelden volgens Keegan in de Kosovo-campagne een ondergeschikte rol: *'All to be said to that is that diplomacy had not worked before March 24, when the bombing started, while the deployment of a large ground force, through clearly a growing threat, would still have taken weeks to accomplish at the moment Milosevic aced in. The revisionists are wrong. This was a victory through airpower'*.¹⁹

Andere analisten stelden deze beslissende rol van de luchtaanvallen ter discussie en relativerden die.²⁰ Zij meenden dat de luchtaanvallen weliswaar van belang waren bij het op de

knieën krijgen van Milosevic, maar dat de luchtaanvallen slechts één van de factoren waren.²¹ Twee andere punten droegen bij aan de verslechtering van de positie van Milosevic. Zo leidde de opbouw van grondtroepen van de NAVO tot extra druk op het regime en daarnaast keerde Rusland, de historische bondgenoot van Servië, Milosevic in het voorjaar van 1999 de rug toe.²² De waarheid ligt vermoedelijk ergens in het midden. Tegelijkertijd geldt dat verdere diplomatieke onderhandelingen waarschijnlijk niet tot stand waren gekomen en dat Rusland zijn positie niet gewijzigd had als er geen luchtaanvallen hadden plaatsgevonden.

Historische context

Als een van de negentien deelnemende NAVO-partners heeft de Koninklijke Luchtmacht een bijdrage geleverd aan het welslagen van Allied Force. Maar is deze bijdrage imposant genoeg om in aanmerking te komen voor een vaandelopschrift? Om die vraag te beantwoorden is nauwgezet de context geanalyseerd waarin de operatie plaatsvond. Dit gebeurde aan de hand van zes punten:

- samenstelling en omvang van de betrokken eenheden;
- wijze van optreden;
- opdracht en uitvoering;
- gevaren waaraan de eenheid werd blootgesteld;
- omstandigheden waaronder de strijd werd gevoerd;
- aard en omvang van de eigen en vijandelijke verliezen.

Centraal staat het optreden van de KLu tussen maart en juni 1999. Gekeken naar de omvang

16 Christ Klep en Richard van Gils, *Van Korea tot Kabul. De Nederlandse militaire deelname aan vredesoperaties sinds 1945* (Den Haag, NIMH/Sdu Uitgevers, 2005) 161.

17 Van Loo, *Crossing the border*, 672.

18 John Keegan, 'Please, Mr. Blair, Never Take Such a Risk Again', in: *The Sunday Telegraph*, 6 juni 1999.

19 Idem.

20 Henriksen, 'Inflexible Response', 825-858.

21 Idem, 825-858.

22 Ronald Havenaar, *Eb en vloed. Europa en Amerika van Reagan tot Obama* (Amsterdam, Van Oorschot, 2009) 150.



FOTO KONINKLIJKE LUCHTMACHT

In totaal voerde de KLu met haar F-16's tijdens Allied Force 1.350 sorties uit

van het optreden valt op dat een substantieel deel van de luchtmacht werd ingezet tijdens de Kosovo-crisis. Eind jaren negentig bestond de totale vloot aan Nederlandse F-16's uit 108 operationeel inzetbare toestellen, verdeeld over zes operationele jachtvliegtuigsquadrons. Bij Allied Force startte Nederland met acht vliegtuigen. Later werden dit er twintig, waaronder veertien F-16 *Mid-Life Update* vliegtuigen, gemoderniseerde toestellen die voor meer taken konden worden ingezet. Het optreden vond in gemengd Nederlands-Belgisch verband plaats: de *Deployable Air Task Force* (DATF). Onder de vlag van de DATF opereerden Nederlandse F-16's afkomstig van drie Nederlandse vliegbases, namelijk Leeuwarden, Twenthe en Volkel. De DATF was gestationeerd op de Italiaanse vliegbasis Amendola. Daar werkten zo'n vijfhonderd militairen, onder wie 310 Nederlanders en 190 Belgen. Ook vanuit Nederland werden er belangrijke bijdragen geleverd. Luchtmachtbases in Nederland speelden een rol in de logistieke ondersteuning. Om de vliegtuigen van voldoende munitie te voorzien, waren Munitie Park Alphen en de inzet van de luchttransportvloot van de KLu van groot belang, terwijl de luchtmachtstaf een coördinerende taak vanuit Nederland vervulde. In totaal voerde de KLu met haar F-16's 1.350 sorties uit. Een F-16 vlieger van de KLu die destijds in het inzetgebied actief was, zou gemiddeld zo'n

vijftien oorlogsmissies vliegen. Een aanzienlijk deel van de inzetbare F-16-vliegers van vliegbases Leeuwarden, Twenthe en Volkel was uiteindelijk betrokken bij de missie.

Naast de F-16's stuurde de luchtmacht twee KDC-10's vanaf Vliegbasis Eindhoven, die dienst deden als tankervliegtuig om de jachtvliegtuigen in de lucht van brandstof te voorzien (*Air-to-Air Refueling*). Daarnaast werden de KDC-10's ingezet als transportvliegtuig. Eenzelfde taak kreeg een Hercules C-130 en een Fokker-60. Voor een betere waarneming (luchtbeeld) leverde Nederland ook zestig militairen aan de *Airborne Early Warning Force* van de NAVO, die met E-3A AWACS-radarvliegtuigen de ogen in de lucht vormde. Tot slot leverde de KLu militairen aan hoofdkwartieren en operatiecentra. Buiten Allied Force stuurde Nederland drie Chinook-helikopters van het 298 Squadron met bijbehorend personeel, zo'n 75 militairen, voor de bescherming van OVSE-waarnemers in Kosovo. Dit detachement maakte deel uit van de zogeheten *Extraction Force* en participeerde in de operaties *Provide Shelter* en *Allied Harbour* in Albanië, dat een grote stroom vluchtelingen uit Kosovo te verwerken kreeg.

Niet helemaal rechtmatig, wel legitiem

Het tweede en derde punt, de wijze van optreden en de opdracht en uitvoering, werden af-

gebakend door het politieke mandaat dat een vredesafdwingende operatie voorschreef. In de *Rules of Engagement* lag het recht op individuele zelfverdediging onder alle omstandigheden duidelijk besloten. Het probleem was alleen dat de VN-Veiligheidsraad niet unaniem achter een resolutie stond waarin gebruik van geweld expliciet was toegestaan. Rusland en China, twee permanente leden van de Veiligheidsraad, lagen dwars. Volgens de letter van de wet was gewapend optreden volkenrechtelijk misschien niet helemaal rechtmatig, maar het was wel legitiem: de Veiligheidsraad was het er wel over eens dat de Kosovo-crisis gezien de etnische zuiveringen, deportaties en moordpartijen moest worden beëindigd. Voor sommige juristen bleef Allied Force lange tijd voer voor discussie, omdat de NAVO zonder rechtsbasis in het volkenrecht offensief optrad tegen een soevereine staat. In Nederland is de missie geen onderwerp geworden van politieke controverse. Een brede meerderheid in de Tweede Kamer steunde de missie en alleen de SP stemde tegen.²³

Gevaren en risico's

Dan de gevaren waaraan de eenheid werd blootgesteld (het vierde onderzoekspunt). De inzet was met grote risico's omgeven. Zo waren doelen lastig te herkennen en dikwijls lagen ze verscholen in bergranden, waren ze ingegraven of gecamoufleerd. Ook de omstandigheden waaronder de KLu moest opereren (het vijfde punt) waren risicovol. De kans op het toebrengen van *collateral damage* was bijvoorbeeld vrij groot. De kans op nevenschade werd per doel van tevoren ingeschat en gekenmerkt door de kwalificaties *high, medium, low of unknown*. Soms lagen de doelen slechts op enkele honderden meters afstand van huizen van burgers. Een andere keer was de informatie minder concreet, maar rees het vermoeden dat op slechts 250 meter afstand van het doel mogelijk een civiel bouwwerk stond. Nederlandse jachtvliegers vlogen opvallend vaak op doelen waarbij de kans op nevenschade als hoog werd ingeschat. Zoals de eerder genoemde manoeuvre van kapiteinvlieger Duivesteijn aantoont, was het risico van onderschepping door de Servische luchtverdediging groot, vooral in het operatiegebied rond Belgrado. Het leger van Milosevic had de

hoofdstad zwaar beveiligd en dat gold ook voor het luchtruim. Het gevaarlijkst waren de geleide wapens (*Surface-to-Air-Missiles, SAM's*) waarmee de Nederlandse vliegers werden bestookt. Deze raketten hadden een groter bereik dan het luchtafweergeschut en konden, eventueel (radar)geleid, op de vliegtuigen worden afgevuurd.

De politieke druk om burgerslachtoffers en onbedoelde schade aan civiele doelen te voorkomen was bij Allied Force groter dan bij voorgaande missies. Toch waren burgerslachtoffers en onbedoelde schade niet altijd te voorkomen. Er is een twaalftal incidenten bekend waarbij burgers per ongeluk zijn gedood, onder meer doordat munitie slecht functioneerde, door pech en inschattingfouten of door het – achteraf bezien – foutief aanwijzen van doelen. Bij geen van deze incidenten was personeel van de Koninklijke Luchtmacht betrokken. De vliegers waren zich bewust van de risico's van collateral damage en de consequenties die hun optreden hadden voor het milieu. Dit besef wordt geïllustreerd door het feit dat planners van tevoren ruim duizend strategische doelen hadden geselecteerd, maar dat de coalitie tijdens de missie, rekening houdend met deze factoren, meer dan de helft van de doelen niet aanviel. Om meer zekerheid te krijgen wat er zich precies rond het doel afspeelde moesten de vliegers lager vliegen, met als risico gemakkelijk ten prooi te vallen aan de luchtafweer. In tegenstelling tot bijvoorbeeld de huidige missie in Afghanistan, werkten de F-16-vliegers niet samen met *Forward Air Controllers* die ter plaatse doelen nauwkeuriger konden observeren.

Ook toen de militaire campagne vorderde slaagde de NAVO er maar niet in het vijandelijke *Integrated Air Defence System (IADS)* uit te schakelen. De vijand op de grond was goed voorbereid op de komst van de NAVO. Al met al kon de alliantie slechts een beperkt luchtoverwicht verkrijgen, wat het operatiegebied voor de KLu-vliegers gevaarlijk maakte. Gedurende de hele missie bleef het risico voor de vliegers

²³ 'Kamer stemt in met aanval Joegoslavië', in: *NRC Handelsblad*, 25 maart 1999.



FOTO KONINKLIJKE LUCHTMACHT

Tijdens Allied Force nam de KLu de LANTIRN-techniek in gebruik, die de vliegers in staat stelde met grotere precisie bommen te richten

vrij hoog. Volgens bronnen binnen de NAVO waren er in totaal 631 vijandelijke SAM-lanceeringen tijdens Allied Force. Soms troffen die raketten doel: twee Amerikaanse gevechtsvliegtuigen en maar liefst negentien *Unmanned Aerial Vehicles* (UAV's) werden naar beneden gehaald. Een onbekend aantal vliegtuigen raakte beschadigd. Naast het gevaar van onderschepping door de Servische luchtverdediging was er ook het risico in botsing te raken met vliegtuigen van bondgenoten. Op sommige dagen waren er boven het relatief kleine inzetgebied zo'n driehonderd NAVO-vliegtuigen actief, vaak onder beroerde weersomstandigheden met slecht zicht. Maar uiteindelijk liep geen van de Nederlandse F-16's substantiële schade op en er gingen geen Nederlandse levens verloren.

Toetsingscriteria vaandelopschrift

Om het vaandelopschrift te verkrijgen moest de Koninklijke Luchtmacht, met inachtneming van de hiervoor geschetste context van de

operatie, voldoen aan een toetsingsnorm. Deze telt vijf criteria:

- voldoet het gewapend treffen aan de definitie van gevecht of gewapende strijd?;
- hebben de betrokken eenheden zich boven andere Nederlandse eenheden onderscheiden?;
- is voldaan aan eisen van moedig, beleidvol en dapper optreden?;
- is de actie toe te rekenen aan een (deel van de) eenheid of aan het samenstel van deelnemende onderdelen?;
- zijn de Conventies van Genève en het Humanitair Oorlogsrecht nageleefd?

Dat er in 1999 sprake was van een gewapend treffen behoeft weinig discussie, maar bij het tweede punt van de toetsingscriteria ligt dat anders. Er waren immers hoegenaamd geen Nederlandse eenheden tot wie de luchtmacht zich kon verhouden en waarvan zij zich dus kon onderscheiden. Er was uitsluitend inzet van de luchtmacht met jachtvliegtuigen, heli-

kopters en tanker- en transportvliegtuigen. Wat echter wel kan worden vergeleken is de inzet van de Nederlandse luchtmacht en de bijdrage van andere NAVO-partners die deelnamen aan Allied Force.

Kwantitatief grote inzet KLu

Het valt op dat Nederland vergeleken met andere landen kwantitatief een fors aandeel leverde. Koploper was de VS met 65 procent van de totale sorties, gevolgd door de Fransen met acht procent. Samen met de Britten stond Nederland op een gedeelde derde plaats met vijf procent van de sorties. Kwantitatief leverde de Koninklijke Luchtmacht dus meer werk af dan bijvoorbeeld Italië (vier procent), Canada (drie procent), Duitsland (twee procent) of Denemarken (een procent). Hier bovenop kwam nog de inzet van Nederlandse tanker-vliegtuigen, die als een van de weinige hun meegenomen vliegtuigbrandstof ook beschikbaar stelden aan andere NAVO-partners. Het Amerikaanse onderzoeksinstituut RAND maakte een evaluatie van de operatie.²⁴ Hierin wordt de Nederlandse luchtmacht, net als de Franse, Duitse en Italiaanse en die van Groot-Brittannië, betiteld als één van de *Key European Air Forces*. RAND vond het Nederlandse optreden op een aantal punten uitblinken. Op het gebied van *Aerial Refueling* (126 sorties) *Combat Air Patrol* (656 sorties) en *Battlefield Air Interdiction* (319 sorties), scoorde de luchtmacht goed ten opzichte van andere landen.²⁵ Het overzicht van RAND is echter onvolledig omdat de inzet van *Precision-Guided Munitions* (PGM's) niet is opgenomen, een wapen waarmee de luchtmacht later in de missie juist zou excelleren. Rob de Wijk komt in zijn *Pyrrus in Kosovo* met een berekening die laat zien dat Nederland meer deed dan de studie van RAND suggereert: 'Afgezet tegen de Europese landen bezette Nederland zelfs de tweede plaats met twintig procent van alle door Europeanen uitgevoerde vluchten. Daarmee leverde Nederland een relatief grote militaire bijdrage aan operatie Allied Force'.²⁶

De forse inzet van Nederland is voor een deel het gevolg van de halsstarrige houding van het Milosevic-regime, dat na de eerste fase van

luchtaanvallen geen duimbreed toegaf. Hierdoor besloot de NAVO door te gaan met het uitvoeren van luchtaanvallen op doelen met een hoge kans op collateral damage. Door dit besluit steeg de behoefte aan PGM's sterk. In de loop van de missie kon de Koninklijke Luchtmacht als een van de weinige deelnemende landen zonder tussenkomst van andere bondgenoten doelrichtmiddelen gebruiken om vijandelijke doelen aan te stralen. Deze zogeheten LANTIRN-techniek (*Low Altitude Navigation and Targeting Infra-Red for Night*) had Nederland in 1998 aangekocht en zou volgens planning eigenlijk pas in 2000 beschikbaar zijn.²⁷ Maar met instemming van het ministerie van Defensie en met hulp van het Pentagon kon de techniek al tijdens Allied Force in gebruik worden genomen. Daar was haast bij geboden: binnen één week werd nieuwe software getest, werden procedures opgesteld en moest dit alles in de praktijk worden getraind. De LANTIRN-techniek stelde de vliegers in staat om met grotere precisie dan voorheen bommen te richten. Ook konden andere vliegers (onder wie NAVO-bondgenoten) 'inhaken' op de doelen die KLu-vliegers hadden aangestraald, mits de F-16 het doel voortdurend bleef aanstralen. Hoewel er technisch grote voordelen zaten aan deze techniek, nam ook het gevaar navenant toe voor de KLu-vliegers, want zij moesten langer in het inzetgebied blijven waardoor zij langer aan gevaar werden blootgesteld. De met LANTIRN-uitgeruste toestellen vlogen ruim honderd oorlogsmisaties en kregen steeds vaker doelen toebedeeld met een hoge kans op collateral damage. Door gebruik van LANTIRN onderscheidde Nederland zich van andere Europese landen die deelnamen aan de NAVO-missie.

De Amerikanen spraken hun waardering voor de Nederlandse bijdrage openlijk uit en dat was niet zomaar een plichtsgetrouw bedankje. Zij waren namelijk vrij kritisch over de deelname van Europese luchtmachten aan Allied

24 John E. Peters, Stuart Johnsen e.a., *European Contributions to Operation Allied Force. Implications for Transatlantic Cooperation* (Santa Monica, RAND, 2001).

25 Idem, 18-51.

26 Rob de Wijk, *Pyrrus in Kosovo* (Amsterdam, Mets & Schilt Uitgevers, 2000) 19.

27 Van Loo, *Crossing the border*, 695-700.

Force. De Europeanen kwamen heel wat tekort, zeiden de Amerikaanse opperofficieren SACEUR Wesley Clark, admiraal James O. Ellis en luitenant-generaal Michael Short op een hoorzitting van het Congres. Anders dan de Amerikanen hadden de bondgenoten te weinig techniek en kennis in huis op het gebied van precisiebombardementen en nachtoperaties. Tegen deze achtergrond van kritiek is het des te opvallender dat juist de Koninklijke Luchtmacht in positieve zin werd genoemd. Generaal Short maakte de opmerking: *'They recognize that they are small dogs, but they want to have a seat at the table. I would use the Dutch as the prime example. A small air force, a proud air force, a competent air force. They have bought their own tankers. They have two modified DC-10s with the Israeli system in the front with mirrors to allow them to refuel their own airplanes. They have LANTIRN-pods. You'll remember on the first night of the war, a Dutch F-16 shot down a MiG-29? A small air force, but a seat at the table. And I knew I could send the Dutch anyplace I had to send them and they'd salute and say, 'Yes, Boss, we'll be there'.*²⁸

De LANTIRN-apparatuur had significante operationele voordelen, maar vergde ook meer moed van de KLu-vliegers

Kwetsbaar

Moed en beleid vormen samen het derde toetsingscriterium. Het staat vast dat Nederlandse vliegers tijdens Allied Force zijn blootgesteld aan risicovolle en gevaarlijke situaties. 'Zeker is dat vliegers van de KLu tijdens missies voor operatie Allied Force in risicovolle, zelfs hachelijke situaties terecht zijn gekomen', aldus de militair-historische analyse. Er was sprake van een duidelijke gevaarzetting, wat blijkt uit de gewaagde actie van kapitein-vlieger Duivesteijn en zijn wingman. De toekenning van de *Vlieger-*

kruizen onderstreept het gevaar waarin de twee hebben verkeerd. Uit het militair-historisch onderzoek van het NIMH blijkt dat de introductie van de LANTIRN-apparatuur weliswaar significante operationele voordelen had, maar dat het tegelijkertijd meer moed van de vliegers vergde. Tijdens een van deze LANTIRN-missies voerde bijvoorbeeld een formatie F-16's 's nachts een aanval uit op een zwaar verdedigde MiG-21 vliegbasis in West-Servië. Door slecht weer konden de F-16's het doel niet goed aanstralen. Om de bewolking uit de weg te gaan moesten de jachtvliegtuigen aanzienlijk lager vliegen dan gebruikelijk. Ze waren daardoor extra kwetsbaar voor luchtafweer. De vier aanvallende Nederlandse F-16's werden, zodra ze waren gedaald, acuut onder vuur genomen door vijandelijk luchtafweergeschut en grondlucht-raketten. Dat weerhield de vliegers er niet van toch hun missie te volbrengen: het bombarderen van een start- en landingsbaan van de vliegbasis. De vliegers met een LANTIRN-pod moesten extra lang in het inzetgebied blijven om het doel aan te blijven stralen voor hun collega-vliegers.

Conventies van Genève

Over het laatste toetsingspunt, het naleven van de Conventies van Genève, lopen de meningen wat betreft het NAVO-optreden als geheel uiteen. Het luchtoptreden is niet zonder meer kritiekloos ontvangen. Niet verwonderlijk is de kritiek van de regering van voormalig-Joegoslavië op het optreden van de NAVO. Maar ook (Servische) NGO's en Amnesty International uitte bezwaren tegen het aanvallen van bepaalde doelen waarbij burgers in onmiddellijke nabijheid verkeerden.²⁹ Veel kritiek oogstte bijvoorbeeld het bombardement op het hoofdkantoor van de staatstelevisie, de Chinese ambassade in Belgrado en het per ongeluk treffen van een passagierstrein in Kosovo (vliegers dachten een verlaten spoorbrug te bombarderen, maar juist op dat moment kwam daar een trein overheen gereden). Er zijn echter geen feiten aangetroffen die aanleiding geven te vermoeden dat KLu-militairen de Conventies van Genève of het Humanitair Oorlogsrecht zouden hebben geschonden. Bij de NAVO-operaties die onbedoeld nevenschade opleverden, waren evenmin

28 General Michael Short testifying at the Oct 21, 1999 Senate Military Hearings. Transcriptie via: <http://archives.econ.utah.edu/archives/marxism/2000w07/msg00330.html>.

29 'Amnesty: NAVO schond oorlogsrecht', *NRC Handelsblad*, 7 juni 2000.



FOTO US DEPARTMENT OF DEFENSE

De Amerikaanse luitenant-generaal Michael Short prees de KLu als een relatief kleine, maar goed uitgeruste luchtmacht met een grote inzetbaarheid

KLu-militairen betrokken. Hoewel de meeste bommen met redelijke precisie doel troffen, scheelde het soms maar een haar of acties van KLu-vliegers zouden per ongeluk toch tot burgerslachtoffers hebben geleid. De nieuwe doelaanstralingsapparatuur en de korte voorbereidingstijd om daaraan te wennen waren hieraan debet. Zo vergat een vlieger een keer een juiste code in te voeren, zodat de bommen van zijn wingman geen doel troffen. Tijdens een ander incident stortte een bom per abuis in een aardappelveld.³⁰

Conclusie

De bijdrage van de Koninklijke Luchtmacht aan de operatie Allied Force laat zien hoe een klein land met een relatief kleine vloot operationele vliegtuigen toch in staat kan zijn een verschil te maken tijdens een internationale missie. Klein maar fijn, lijken de Amerikanen te willen zeggen in hun appreciatie van het Nederlandse optreden. Voor Nederlandse begrippen was de missie overigens helemaal niet zo klein.

In totaal hebben Nederlandse F-16's 852 bommen en raketten (bij elkaar opgeteld 430 ton wapens) afgeworpen of afgeschoten. Van deze wapens waren er 574 niet-precisie en 278 wel precisie-geleid. De vliegers waren zowat volcontinu aan het werk. In een interview zei kapitein-vlieger Duivesteijn: 'Het was geen vijf dagen werken, twee dagen vrij. (...) In die twee maanden heb ik één weekend vrij gehad. Vooral de eerste periode betekende dat hard werken. Tot het einde van de vijandelijkheden op 10 juni heb ik elke dag gewerkt op dat ene weekend na. Dat gaat aan je vreten (...) Je bent na verloop van tijd moe, het lontje wordt steeds korter en je tenen steeds langer. Kortom: je raakt snel geïrriteerd. Lichamelijk ben je helemaal op, en psychisch ook eigenlijk. Zo'n weekend vrij blijkt dan toch te kort om bij te tanken'.³¹

De ervaringen van Marcel Duivesteijn en veel van zijn luchtmachtcollega's tonen aan dat de KLu bij de inzet in de Kosovo-crisis te maken had met een duidelijke gevaarstelling. De toekenning van het vaandelopschrift 'Kosovo 1999' doet daarom recht aan het onderscheidende optreden van de luchtmacht tijdens operatie Allied Force. ■

30 Van Loo, *Crossing the border*, 704.

31 Idem, 704-705.

Cybersecurity

Relevante trends voor Defensie

Wereldwijd stijgt het aantal incidenten door cybercriminaliteit sterk. Door computers te besmetten kunnen criminelen deze computers inzetten voor eigen gewin. Hier worden miljoenen mee verdiend. Geleidelijk aan raken steeds meer zakelijke en privé computers besmet met virussen en wordt ontsmetting moeilijker. Daarnaast professionaliseert de cybercriminaliteit. De strijd tussen verdedigers en aanvallers is inmiddels een wedloop geworden. Kennis van het cyberdomein is voor de defensieorganisatie essentieel, omdat ze sterk afhankelijk is van informatiesystemen. Software met een groot marktaandeel is extra aantrekkelijk voor cybercriminelen. Het zou daarom goed zijn als Defensie de huidige IT-monocultuur doorbreekt door diversiteit te bevorderen en meer gebruik te maken van 'open source'-systemen.

H.J. van der Molen*

Sinds 27 juni 2012 heeft Defensie een cyberstrategie. Hiermee onderkent zij de noodzaak van een effectieve inzet van digitale middelen om haar hoofdtaken uit te kunnen voeren.¹ De hoofdtaken uit deze strategie zijn als volgt samengevat: het beschermen van de vitale belangen van Nederland, het bevorderen van de (inter)nationale rechtsorde en het ondersteunen van civiele autoriteiten bij de bestrijding van rampen, zowel in nationaal als internationaal verband.

Behalve de capaciteit om effectief te kunnen opereren in het cyberdomein, moet Defensie dus ook adequaat en proportioneel kunnen reageren op cyberaanvallen die Nederlandse vitale belangen bedreigen of rampen (kunnen) veroorzaken. Daarnaast onderstreept de cyberstrategie dat Defensie zowel defensieve als offensieve cyberacties moet kunnen uitvoeren.

Inleiding

Of een cyberincident wordt beschouwd als een cyberaanval wordt onder meer bepaald door de impact. Zowel bij een cyberincident als bij een cyberaanval is het moeilijk om de inbraak te signaleren, de ingezette middelen vast te stellen, de aanvaller te identificeren en diens intentie vast te stellen. Doordat de meeste *malware* (een verzamelnaam voor programmatuur met een kwaadaardige functionaliteit) elke kwetsbare computer probeert te besmetten is het zelfs voor de makers moeilijk om de impact van hun malware te voorspellen.

Defensie is sterk afhankelijk van informatiesystemen die bijvoorbeeld de commandovoering ondersteunen. Het is inmiddels bewezen dat ook militaire systemen die de *Observe-Orient-Decide-Act* cyclus ondersteunen kwetsbaar zijn voor cyberaanvallen.²

Defensie moet kunnen beschikken over voldoende cyberkennis om het cyberrisico voor de eigen systemen te verminderen en om mee te kunnen denken over de bescherming van Nederlandse (civiele) vitale systemen.

* De auteur is freelance docent bij de Hogeschool Wageningen, onder meer op het gebied van informatiebeveiliging, *business intelligence*, verandermanagement en strategisch IT-management. Hij heeft diverse artikelen gepubliceerd op ICT-gebied en geeft regelmatig lezingen.

1 *Defensie Cyber-strategie*: www.rijksoverheid.nl.

2 Zie bijvoorbeeld hoofdstuk 4 'The Defense fails', in: *Cyber War*, R.A. Clarke.

Opzet artikel

Ik ga eerst in op trends van cyberincidenten en een economische model achter cyberaanvallen. Op basis daarvan geef ik aan waarom het risico van cyberincidenten moeilijk te verminderen is, onder welke omstandigheden dat risico het grootst is en welk effect beveiligingsmaatregelen hebben. De problematiek speelt voor zowel organisaties als Defensie als voor individuele computergebruikers. Het artikel is bedoeld voor beleidsmakers, IT-personeel en defensiemedewerkers. De context is waar mogelijk toegesneden op Defensie. Ik rond af met conclusies en aanbevelingen.

De kans op besmetting met malware

In de civiele wereld stijgt het aantal cyberincidenten momenteel sterk, vooral door de inzet van malware. Door computers met malware te besmetten kunnen cybercriminelen deze computers ongemerkt voor eigen gewin inzetten (zie tabel 1).

In 2010 bevatte 1 op de 284 e-mails (0,35 procent) malware. In 2011 nam dat toe tot 1 op 239

e-mails (0,42 procent) en steeg het aantal unieke malware-varianten met 41 procent tot 403 miljoen.³ De criminele bedrijfstak rond malware groeit, omdat er miljoenen mee verdiend worden.⁴ Bijvoorbeeld door verkoop van gevoelige bedrijfsinformatie, chantage, afpersing, frauderen met creditcardgegevens en click-fraude met online advertenties.

Steeds meer financiële schade

Cybercrime veroorzaakt hierdoor steeds meer financiële schade voor personen, organisaties en de samenleving als geheel. Daarnaast neemt de dreiging van een cyberaanval op vitale systemen toe. Al in 2003 was een alarmpaneel van een Amerikaanse nucleaire installatie vijf uur lang onbruikbaar omdat dit systeem met een worm was besmet.⁵

- 3 MessageLabs Intelligence: 2010 Annual Security Report, 7 december 2010: www.clear-northtech.com; Internet security Threat Report 2011 Trends, www.symantec.com.
 4 'How Cybercriminals Make Their Millions': www.esecurityplanet.com, 22 december 2010.
 5 Informatiebeveiliging juni 2008, 'Beveiliging procescontrole is onderbelicht onderwerp', Eric Luijff, www.pvib.nl.

Categorie	Beschrijving	Mogelijke acties malware
Computer virus	Kan zichzelf vermenigvuldigen en verspreiden naar andere computers, bijvoorbeeld door koppelen aan bestaande software	<ul style="list-style-type: none"> Bestanden downloaden, aanpassen of verwijderen Schermafdrucken maken
Computer worm	Een op zichzelf staand computerprogramma, dat zich kan verspreiden naar andere computers binnen hetzelfde netwerk	<ul style="list-style-type: none"> Toetsaanslagen registreren (wachtwoorden!) Op afstand de microfoon of de camera inschakelen
Trojaans paard	Malware vermomd als nuttige software, zoals anti-virussoftware	<ul style="list-style-type: none"> Mail (spam / malware) versturen Privacygevoelige informatie uploaden
Bot	Door een 'achterdeurtje' heeft de aanvaller via het internet volledige controle over alle besmette computers in zijn 'botnet'. Het 'Zwitserse zakmes' van de cybercrimineel	<ul style="list-style-type: none"> (verborgen) Accounts aanmaken Besmetten verbonden computers via netwerk, USB-drives en Bluetooth
Spyware	Stuurt identiteitsgegevens (zoals wachtwoorden en creditcard-gegevens) van de computergebruikers door naar de aanvaller	<ul style="list-style-type: none"> Communicatie afluisteren
Rootkit	Software met beheerdersrechten die zich verborgen kan houden voor normale detectiemiddelen, zoals anti-virussoftware	

Tabel 1. Verschillende soorten malware

Cybercriminelen kunnen computers met malware infecteren door kwetsbaarheden in de software te misbruiken.⁶ Elk gedownload computerprogramma kan malware bevatten, maar ook bestanden met macro's, beeld, geluid of video. Een computer kan zelfs al een malware-besmetting oplopen door één besmette website te bezoeken.

Een Amerikaans beveiligingsbedrijf constateerde in 2009 dat 60 procent van de onderzochte websites tenminste één ernstig beveiligingslek heeft.⁷ In 2010 werden gemiddeld 3188 malafide sites per dag geblokkeerd, waarvan bijna 90 procent legitieme sites die waren gehackt. In 2012 had Nederland – na Rusland en de VS – de meeste websites die malware verspreiden.⁸

Ongerichte aanvallen

Hoewel malware-aanvallen soms worden gericht op individuele personen of organisaties, probeert de meeste malware ongericht alle systemen te besmetten waarmee het in contact komt. Cybercriminelen zijn geneigd om malware voor gerichte aanvallen waarmee geld werd verdiend, ook elders in te zetten. Malware is daarom afhankelijk van (kwetsbaarheden in) bepaalde software om zich te kunnen verspreiden naar onbesmette systemen.

Informatietechnologie (IT) maakt nog steeds een explosieve groei door en ijlt soms na op de ontwikkelingen. Daardoor bevat alle software fouten of kwetsbaarheden die een cyberaanval mogelijk maken. Van de kwetsbaarheden die bijvoorbeeld tussen juli 2011 en maart 2012 bekend werden, blijkt 55 procent relatief eenvoudig uit te buiten en is circa 90 procent van de kwetsbaarheden vanaf het internet uit te buiten.⁹

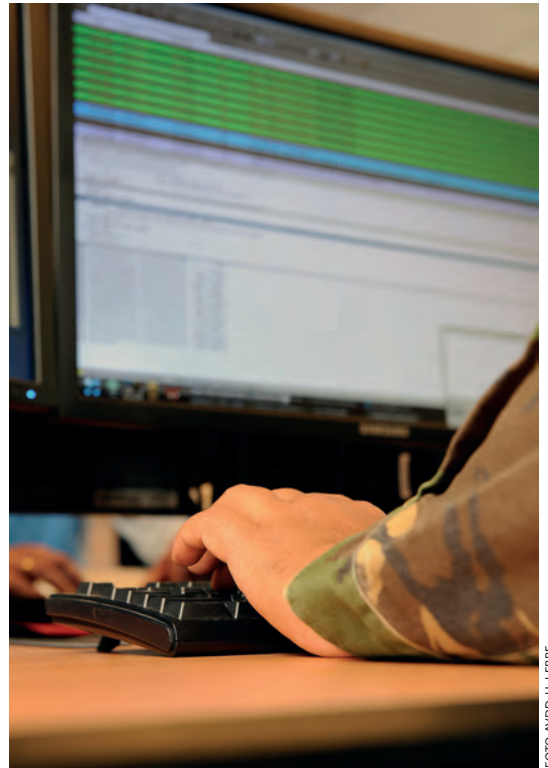


FOTO AVDD, H. LEBBE

Informatietechnologie maakt nog steeds een explosieve groei door. Defensie is sterk afhankelijk van informatiesystemen, bijvoorbeeld voor het ondersteunen van de commandovoering. Hierdoor is Defensie kwetsbaar voor cyberaanvallen

Om fouten in hun software te repareren verspreiden leveranciers updates (*patches*) via internet. In 2010 werd tot dan toe het grootste aantal kwetsbaarheden in software gepubliceerd, terwijl 44 procent van alle aan het licht gekomen kwetsbaarheden niet kon worden gerepareerd voor het einde van dat jaar. 95 procent van deze kwetsbaarheden werd geclassificeerd als 'medium zwaar'.¹⁰

Door een uitgebrachte software-update te vergelijken met de oude software kan men eenvoudig signaleren welke kwetsbaarheden de update repareert. Het is een Amerikaanse universiteit gelukt om uit een software-update automatisch de malware te genereren die niet-geüpdate computers kan aanvallen.¹¹ Het vermoeden wordt steeds sterker dat cybercriminelen deze procedure stelselmatig kunnen toepassen. Zo werd in 2009 circa 60 procent van de gemelde kwetsbaarheden actief misbruikt.¹²

6 In dit artikel worden de termen 'malware' en 'exploits' gebruikt als synoniemen; meestal misbruikt een exploit een kwetsbaarheid in software en kan daardoor malware downloaden en installeren

7 'WhiteHat Security Statistics Report', 18 mei 2009, www.whitehatsec.com.

8 'Kaspersky Lab, IT threat evolution Q3 2012', 1 november 2012, www.securelist.com.

9 'Cyber Security Beeld Nederland' (CSBN-2) juni 2012 (nscs.nl), www.nctb.nl.

10 'Symantec Corp., Internet Security Threat Report' Vol. 16, april 2011, www.symantec.com.

11 *Automatic Patch-Based Exploit Generation*, Carnegie Mellon University, UC Berkeley, CMU, U. Pittsburgh, 2008, www.cs.cmu.edu.

In 2011 verslechterde deze situatie: ongeveer 97 procent van alle kwetsbaarheden werd binnen twee weken na publicatie misbruikt.

Vrij spel

Totdat de kwetsbaarheden worden gerepareerd, heeft malware vrij spel. Zodra een software-leverancier een update uitrolt, moeten gebruikers van deze software die zo snel mogelijk installeren. Hoe langer het duurt om kwetsbaarheden te repareren, des te groter de kans dat kwetsbare systemen ondertussen met malware worden besmet. Organisaties lopen soms achter bij het doorvoeren van updates, bijvoorbeeld omdat ze de uitgebrachte updates eerst willen testen of door slecht systeembeheer. Helaas komt dat laatste vaak voor: de zogeheten 'SQL Slammer'-worm met de bijbehorende reparatie-update verschenen al in 2003. Toch genereerden de systemen die nu nog met deze malware zijn besmet in 2010 het meeste verkeer van alle malware op het internet.

Uit onderzoek blijkt dat cybercriminelen steeds sneller malware kunnen ontwikkelen omdat hun kennis van IT toeneemt en omdat ze onderling samenwerken.¹³ Al in 2003 werd bijvoorbeeld voor het schrijven van de succesvolle 'Sobig'-worm universitaire kennis ingezet, zijn delen van andere malwarevarianten hergebruikt en zijn er verschillende testversies uitgebracht.¹⁴

Zwarte markt

Op de zwarte markt wordt malware verkocht, ook voor de nieuwste systemen. Een netwerk met 10.000 besmette pc's is ongeveer \$ 800,- waard en kan per uur worden gehuurd, bijvoorbeeld om spam te versturen of een webwinkel plat te leggen en zo geld af te persen.¹⁵ De 'Storm'-worm malware heeft naar schatting anderhalf miljoen computers besmet; deze malware zou in 2007 20 procent van alle spam wereldwijd hebben verstuurd. Het 'Conficker'-virus kon in 2008 miljoenen besmette pc's flexibel inzetten doordat het virus nieuwe versies van zichzelf kon installeren.¹⁶ In 2011 registreerde een beveiligingsbedrijf tot zijn verrassing 1,2 miljoen pc's die waren besmet met de 'Ponmocup'-malware – in 24 uur.¹⁷

Het is bekend dat medewerkers de meeste incidenten binnen organisaties veroorzaken. De gemiddelde computergebruiker weet weinig over beveiliging, waardoor privécomputers vaak en langdurig besmet zijn. Veel mensen gebruiken bijvoorbeeld thuis dezelfde kantoorsoftware als de zakelijke standaard. Als organisaties deze software niet gratis verstrekken, downloaden veel mensen illegale software, die vaak besmet is met malware. Bovendien verbeteren cybercriminelen continu hun zogeheten *social engineering*-technieken om personen te verleiden tot onveilig gedrag.¹⁸ Als ondeskundigen malware langer in omloop houden is dat ook nadelig voor goed beveiligde systemen met dezelfde kwetsbaarheden. Omgekeerd is het beter beveiligen van computers van ondeskundige eigen medewerkers ook voordelig voor de organisatie.¹⁹

Defensie

Defensie doet er goed aan om de privécomputers van medewerkers te beschouwen als mogelijk besmet met malware. Als een medewerker op zijn besmette computer thuis werkt aan een zakelijk document kan bedrijfsinformatie naar buiten lekken. De oplossing met de telestick van Defensie maakt het buitmaken van bedrijfsinformatie wel een stuk moeilijker maar niet onmogelijk (zie tabel 1). Daarnaast moeten medewerkers zich ervan bewust zijn dat een aanval op hun organisatie kan starten vanaf hun privécomputer. Zakelijke computers en privécomputers van medewerkers zijn vaak direct gekoppeld via e-mail en USB-drives. Dergelijke koppelingen kunnen malware overdragen. Voor de hand liggende maatregelen

12 Fortinet, Threatscape Report, juni 2009, www.fortiguard.com/report/roundup_june_2009.html

13 P. Bueno, 'Malware Analysis—Lessons Learned', SANS Internet Storm Center, <http://handlers.sans.org>.

14 'Who wrote the Sobig?', Author Travis Group, 2003-2004, <http://spamkings.oreilly.com>.

15 Zie www.security.nl/artikel/30701/1/Besmette_Windows_computer_10_cent_waard.html

16 'Midyear Security Report: An Update on Global Security Threats and Trends', Cisco Systems Inc., 2009, www.cisco.com.

17 'How Big is Big? Some Botnet Statistics', 23 mei 2011, www.abuse.ch/?p=3294.

18 Social Engineering Fundamentals, Part I: Hacker Tactics, www.symantec.com.

19 'On the Malware Front', R.E. Kooij, H.J. van der Molen, *International Journal of Computer Networks (IJCN)*, 4 (4) (2012) <http://cscjournals.org>.

zijn dan vreemde USB-apparaten te weren op de werkplek, en thuiswerken alleen toe te staan op zakelijke hard- en software.

Beveiliging is geen garantie

Steeds meer organisaties koppelen systemen aan het internet (Web 2.0), zoals internet-banken, webshops en online nutssystemen. Dit vergroot de kans dat malwarebesmettingen bedrijfsprocessen verstoren. Ook de overheid loopt meer risico: de ambitie was om in 2007 minstens 65 procent van de dienstverlening via internet te laten lopen. Het aantal gekoppelde overheidssystemen neemt verder toe door het wettelijk verplichte gebruik van Nederlandse basisregistraties, zoals de GBA en het KvK-register. Door de toename van systemen, centralisatie en uniformering van software lijken ICT-infrastructuren steeds meer op elkaar en neemt de afhankelijkheid van ICT toe.²⁰

Grote organisaties zoals Defensie hebben hun computersystemen vaak beter beveiligd, bijvoorbeeld doordat medewerkers zelf geen software kunnen installeren. Daarom lijken incidenten met malware voornamelijk voor te komen bij individuele computergebruikers of kleine bedrijven, maar dat beeld is niet representatief. Het blijkt dat 16 procent van de Nederlandse organisaties al in 2008 last hadden van incidenten met malware.²¹ In de VS was 50 procent van de cyberaanvallen (in 2011) gericht op organisaties met meer dan 2500 medewerkers. 42 Procent van de zogeheten *spear phishing* aanvallen (persoonlijke e-mails van een 'kennis') werd gericht op seniormanagers en R&D-personeel.

Gerichte aanvallen

Overheden en de publieke sector kregen in 2011 25 procent van deze gerichte e-mail-aanvallen. Ook de systemen van de 'Fortune 500'-bedrijven zijn gehackt.²² In 2011 maakten aanvallers de details buit van het zogeheten RSA-beveiligingssysteem, dat miljoenen medewerkers gebruiken om thuis veilig te kunnen werken. Zelfs de FBI gaf in maart 2012 aan dat de verdediging van IT-systemen niet is opgewassen tegen de tools die aanvallers gebruiken.²³

Organisaties detecteren bovendien niet alle inbraken op hun systemen, bijvoorbeeld bij bedrijfsspionage. Ook doen weinig organisaties aangifte van cyberaanvallen omdat ze negatieve publiciteit willen vermijden. Inbraken die leiden tot een faillissement vormen echter geen uitzondering meer.²⁴ Hoewel de veiligheidsmaatregelen verschillen tussen de diverse organisaties en landen kunnen geslaagde aanvallen vaak met succes worden hergebruikt. Medewerkers en managers zijn zich vaak onvoldoende bewust van de waarde van de informatie waarover zij beschikken en het belang van informatiebeveiliging.

Daarom vraagt de AIVD sinds 2010 organisaties nadrukkelijk om een KWetsbaarheids Analyse Spionage (KWAS) uit te voeren en maatregelen te nemen.²⁵

Wedloop

De strijd tussen verdedigers en aanvallers is een wedloop (zie de voorbeelden van acties en tegenacties in tabel 2). Zelfs een ICT-infrastructuur met de veiligste instellingen is niet immuun voor alle malware-aanvallen.²⁶

De maatregelen tegen malware blijken namelijk steeds minder effectief om incidenten te voorkómen. Zo wordt er regelmatig malware gevonden die kwetsbaarheden misbruiken, waartegen nog geen beveiligingsmaatregel bestaat, de zogeheten *Zero-day exploits*.²⁷ Ook beveiligingsmaatregelen zoals 'twee factor authenticatie' (naast een wachtwoord een *security token* invoeren, zoals bij internet-bankieren of telewerken) is niet opgewassen tegen de nieuwste malware.

20 De rijksoverheid wil met het plan 'Compacte Rijksdienst' het aantal rekencentra terugbrengen van 64 naar vier à vijf.

21 'Resultaten ICT Barometer Over ICT-beveiliging en Cybercrime', Ernst & Young, 28 januari 2009, op www.ict-barometer.nl.

22 CNN, 28 oktober 2011 'Massive hack hit 760 companies', <http://money.cnn.com>.

23 'U.S. Outgunned in Hacker War', <http://online.wsj.com>.

24 'DigiNotar failliet verklaard', *NRC Handelsblad*, 20 september 2011, www.nrc.nl.

25 'Weerbaarheid overheid en bedrijfsleven tegen spionage wordt vergroot', <https://www.aivd.nl>.

26 Incident Management broodnodig', *Computable*, 26 mei 2006; zie ook Govcert Trendrapport 2007

27 SearchSecurity.com, 'Exploit Code Targets Internet Explorer Zero-day Display Flaw', 23 november 2009; 'Microsoft Word Zero-day Being Actively Exploited', 8 juli 2008.

Beveiliging tegen malware	Tegenacties cybercriminelen
<p>Verlagen besmettingskans Antivirussoftware, firewall, sterke wachtwoorden, beperkte gebruiksrechten, periodieke veiligheidsonderzoeken, betere beveiligingskennis</p> <p>Verbeter ontsmetting (detectie & correctie) Logging, Incident Management-procedures, betere beveiligingskennis, 'post mortem' onderzoeken</p>	<p>Verhogen besmettingskans Testen van malware, gerichte malware, imitatie van legale software, malware op vertrouwde websites, encryptie malware</p> <p>Bemoeilijk ontsmetting Encryptie communicatie, malware update sneller dan antivirussoftware, malware wist de sporen, continuïteitsplan voor botnets</p>

Tabel 2. De wedloop tussen cybersecurity en cybercrime

Ook overheden zijn betrokken bij cyberaanvallen, zoals Rusland tegen Estland in 2007. In juni 2010 is het Stuxnet-virus ontdekt. Dit virus wordt beschouwd als het eerste strategische cyberwapen. Het kon specifieke Siemens-systemen saboteren die onder meer in Iran werden gebruikt voor nucleaire ultracentrifuges. Het Stuxnet-virus vermenigvuldigde zich onder meer via USB-drives en verborg zijn aanwezigheid op besmette computers. Het virus bevatte meerdere Zero-day exploits en een softwarecomponent die ondertekend was met gestolen certificaten.

Op basis van deze complexiteit schat men de benodigde tijd om Stuxnet te ontwikkelen op circa tien manjaren. Sinds 2010 staan de ontwikkelingen echter niet stil: de opvolgers van Stuxnet zijn al gesignaleerd.²⁸ De AIVD signaleerde in april 2011 dat de digitale spionage van onder meer China en Rusland toeneemt. Bij een destructieve cyberaanval in augustus 2012 werden er alleen al bij het Saoedische energiebedrijf Aramco meer dan 30.000 werkstations besmet. Op basis van de fouten in het virus worden de ontwikkelaars aangemerkt als 'getalenteerde amateurs'.²⁹ Ook cybercriminelen en anarchisten richten zich steeds meer op het hacken van industriële systemen die bijvoorbeeld kerncentrales, waterbedrijven en sluisen aansturen.³⁰

Professionalisering van cybercrime

Criminelen willen ook in crisistijd veel geld verdienen, en cybercrime met zijn anonieme slachtoffers is dan een aantrekkelijke optie. Om de verdienste te maximaliseren moet malware verborgen blijven, moet de verspreiding van malware 24/7 doorgaan en moet een besmetting met malware zo lang mogelijk duren. Daarvoor worden bijvoorbeeld encryptie en roulerende webservers ingezet, zodat het uitschakelen van enkele servers weinig effect heeft.

Virusscanners

Al in 1992 was bekend dat detectiesystemen nooit de afwezigheid van alle malware kunnen aantonen; alleen de afwezigheid van bekende malware.³¹ Cybercriminelen verifiëren tegenwoordig voorafgaand aan de verspreiding dat virusscanners hun malware niet herkent. Door voor elke besmetting unieke malware te genereren en deze selectief te richten op enkele organisaties verschijnt nieuwe malware niet

28 F-Secure 2 juni 2012, 'On Stuxnet, Duqu and Flame', www.f-secure.com.

29 'Shamoon Malware and SCADA Security – What are the Impacts', 25 oktober 2012, <https://www.tofinosecurity.com>.

30 'Hackers richten pijlen op kerncentrales', *Webwereld*, 26 oktober 2012, zie: <http://webwereld.nl>.

31 'Defense in Depth against Computerviruses', Cohen, F.B., *Computers & Security* 11 (6) 1992.

meer op de radar van de leveranciers van anti-virussoftware. Volgens verschillende onderzoeken laten zelfs up-to-date virusscanners circa 60 procent van alle nieuwe malware door.³²

Mede vanwege de tijd die nodig is om nieuwe antivirussoftware uit te rollen detecteren virusscanners in de regel pas malware als die meer dan vier weken oud is. Er circuleert al malware die niet gedetecteerd kan worden, omdat die sneller updates ophaalt van het internet dan dat virusscanners worden bijgewerkt. Het zogeheten heuristisch scannen – het bepalen van de waarschijnlijkheid dat een bestand een virus bevat – biedt hiervoor geen goede oplossing: het leidt tot (te) veel valse positieven. Dat zowel commerciële software als malware vaak is ingepakt in gecompakteerde zip-bestanden maakt de detectie van malware veel moeilijker. Sommige virusscanners kunnen malware detecteren aan de hand van het gedrag, maar dan is het systeem al besmet en is de veiligheidsssoftware mogelijk al uitgeschakeld. Natuurlijk bestaan er meer geavanceerde beveiligingssystemen, maar die hogere effectiviteit vergt een groot budget en veel kennis. Ook voor dergelijke systemen kunnen geen garanties worden afgegeven.

Lage pakkans, hoge inkomsten

Mensen die aangifte doen van computercriminaliteit merken vaak dat de daders niet worden veroordeeld, omdat het achterhalen van de daders moeilijk is, cyberbendes meestal vanuit het buitenland opereren en er alles aan doen om de dans te ontspringen. Door de lage pakkans en hoge inkomsten laat het aantal malwareprogramma's een exponentiële groei zien.³³ Het aantal virussen is zo groot omdat *one click* viruskits op het internet weinig of geen geld kosten en omdat criminelen hetzelfde virus opnieuw kunnen gebruiken door deze verspreiden met een unieke sleutel.

Antivirus-softwareleverancier Kaspersky meldde al in 2006: *'We're losing this game. There are just too many criminals active on the Internet underground, in China, in Latin America, right here in Russia. We have to work all day and all night just to keep up'*.³⁴ Het beveiligingsbedrijf F-Secure meldde daarna dat de hoeveelheid malware in 2007 verdubbelde en in 2008 nog eens verdriedubbelde. Vanwege de grote hoeveelheid malware die in omloop is, komt het regelmatig voor dat computers besmet zijn met meerdere virussen tegelijk.

Malware is gericht op het marktaandeel van de software

Aan het hand van deze gegevens kan het economische model van malware worden bepaald. Bijna alle software bevat kwetsbaarheden die uitgebuit kunnen worden door malware. Cybercriminelen moeten blijven investeren in de ontwikkeling van malware omdat ze continue nieuwe kwetsbaarheden moeten zoeken en de ontwikkelingen van antivirussoftware vóór moeten blijven. Omdat cybercriminelen de kans willen maximaliseren dat ze die investering terugverdienen is hun inkomstenmodel samen te vatten met de volgende stelling:

Stelling 1 – Professionele cybercriminelen maximaliseren de 'return-on-investment' van hun malware ($P \times Q$) door te focussen op Kwantiteit (Q), niet op de Prijs (P) per besmette computer

Hierbij staat Q (Kwantiteit) voor het aantal computers dat per malware-aanval wordt besmet en P (Prijs) voor de gemiddelde opbrengst per gehackte computer. Focussen op P vergt specifieke voorkennis en biedt minder zekerheid. Het kraken van één systeem met waardevolle bedrijfsgegevens kan weliswaar veel geld opleveren, maar dergelijke systemen zijn vaak goed beveiligd.

Focussen op kwantiteit biedt meer zekerheid qua inkomsten omdat veel computers onvoldoende zijn beveiligd. Bovendien is het eenvoudiger om te kraken.

32 'Do Anti virus Products Detect Bots?', Stanford, S., FireEye Malware Intelligence Lab, 20 november 2008, <http://blog.fireeye.com>. Zie ook *Retrospective/Proactive Test, AV-Comparatives.org, May 2011*, www.av-comparatives.org.

33 F-Secure, 'F-Secure IT Security Threat Summary for the Second Half of 2008', www.f-secure.com.

34 'The Zero-Day Dilemma', Naraine, R., eWeek.com, 24 januari 2007, www.eweek.com.

Categorie	Softwareproduct	Markt % (schatting)	Datum en bron schatting	Populariteit bij criminelen
Office suite	MS Office	88 (v)	mei 2010 Webmasterpro.de	zeer hoog
Operating system	Windows	85 (i)	mei 2012 Marketshare.com	zeer hoog
Web client	Internet Explorer	54 (i)	mei 2012 Marketshare.com	zeer hoog
Web server	Apache	65 (i)	januari 2012 Netcraft	hoog
Database server	Oracle	49 (v)	maart 2012 Gartner	hoog

(v = aantal verkocht, i = internet onderzoek)

Tabel 3. Marktaandeel software en aantrekkelijkheid voor cybercriminelen

diger omdat alleen informatie nodig is over de verhoudingen in de softwaremarkt. Bijkomend voordeel is dat als er duizenden gedupeerden aangifte doen van een kleine diefstal, vervolging voor justitie moeilijker is dan wanneer één partij aangifte doet van een groot misdrijf.

Volgens het *Nationale trendrapport Cybercrime en Digitale Veiligheid 2010* bestaan er in Nederland monoculturen voor pc-besturingssystemen, webbrowsers, pdf-readers en Adobe Flash.³⁵ Veel cyberbendes richten hun malware op de software die op dat moment marktleider is. Ze kunnen deze producten gewoon kopen, om daarna uitgebreid te testen welke kwetsbaarheden ze kunnen misbruiken. Malware voor deze software levert het meeste op, omdat in de beschikbare tijd (van de uitrol van de malware tot de 'ontsmetting') de meeste systemen worden besmet. Deze strategie maximaliseert ook de kans dat gerichte malware kan worden hergebruikt. Het marktaandeel bepaalt dus welke software cyberbendes onderzoeken op kwetsbaarheden. In tabel 3 staat per categorie het dominante softwareproduct.

Op veel computers van Defensie en de thuiscomputers van defensiemedewerkers draait software van marktleiders, bijvoorbeeld Microsoft. Door de commercialisering en professionalisering van cybercrime kan iedere partij die een cyberaanval wil lanceren, daarvoor vrij eenvoudig de benodigde deskundigen, de kennis en de middelen inkopen. Defensie moet dus regelmatig haar informatiesystemen onder-

zoeken om inbraken tijdig te kunnen detecteren, om hacken zo moeilijk mogelijk te maken en om de impact van een geslaagde aanval te minimaliseren.

Erop vertrouwen dat beveiliging superieur is en alle besmettingen kan voorkomen, is niet meer realistisch. Organisaties moeten een plan maken voor wat hen te doen staat als hun systemen besmet raken. Zo'n *Incident Response Plan* vermindert de impact van een besmetting, maar alleen als dit plan regelmatig wordt getest op actualiteit en effectiviteit.

Het kiezen van software

Uit diverse onderzoeken blijkt dat het marktaandeel van een softwareproduct niet correleert met het aantal gesignaleerde kwetsbaarheden. Wel lijkt er een sterke relatie te bestaan tussen het marktaandeel en de hoeveelheid malware in omloop.³⁶ IBM stelt dat het veelgebruikte *Common Vulnerability Scoring System* blind is voor de economische motieven van hackers om software te kraken.³⁷ Dit klopt met het veelgehoorde argument dat de grote hoeveelheid malware voor bijvoorbeeld Windows, voornamelijk ligt aan het hoge marktaandeel en minder aan de vaak bekritiseerde kwaliteit van die software.

³⁵ Het trendrapport 2010 is te vinden op www.govcert.nl.

³⁶ Know Your Enemy: Malicious Web Servers, The HoneyNet Project, 7 augustus 2007, www.honeynet.org.

³⁷ IBM Global Technology Services, IBM Internet Security Systems: X-Force® 2008 Trend & Risk Report, January 2009, www-935.ibm.com.



FOTO AVDD, W. SALIS

Softwareproducten met een groot marktaandeel, zoals Microsoft, zijn aantrekkelijk voor cybercriminelen. Meer diversiteit in IT is daarom wenselijk. Op de foto: het 'Network Operations Centre' van IVENT

Kwaliteit

De kwaliteit van software wordt vaak aangeduid met het aantal fouten per duizend regels programmacode. De complexiteit en omvang van een computerprogramma bepalen het aantal fouten en daarmee de kansen voor malware. De kwaliteit van verschillende softwarepakketten objectief vergelijken is om verschillende redenen lastig. Zeker als de programmacode niet openbaar is, moeten moeizame voorzorgsmaatregelen worden getroffen om ervoor te zorgen dat niet-openbare programmacode geheim blijft.

Bedrijven die gesloten software verkopen willen meestal zelf de *reviewers* selecteren, eisen van hen geheimhouding en beïnvloeden de onderzoeksresultaten. Daarnaast zijn onderzoeksrapporten van gesloten software direct verouderd zodra er een nieuwe versie op de markt komt.

'Open source' software

Dat cybercriminelen de programmacodes van open software (de zogeheten 'open source soft-

ware') kunnen naspeuren op kwetsbaarheden, beschouwt men over het algemeen niet als een hoger veiligheidsrisico. Dat komt omdat open source producten in alle openheid worden gebouwd en getest. In een interne studie van Microsoft staat dat open source softwareprojecten het niveau van commerciële software kunnen evenaren of zelfs overtreffen.³⁸ Openbare reviews maken objectief duidelijk of producten al dan niet veilig genoeg zijn. Zo is de AES encryptie, bekend van Winzip, destijds ontwikkeld als open technologie. Bovendien blijkt altijd achteraf dat vertrouwen op de geheime werking van een systeem (*security by obscurity*) onterecht is.³⁹

Daarnaast wordt open source software vaak genoemd om de snelle reparatie van tekortkomingen. Deze snelheidswinst is mogelijk doordat de programmacode van alle versies openbaar is, en iedereen suggesties voor verandering direct in programmacode formaat kan aanleveren. Dit voordeel geldt overigens alleen voor open source producten met een actieve ontwikkelgroep.

Op basis van een ander onderzoek neemt men aan dat het aantal kwetsbaarheden voor open en gesloten source software per kilobyte programmacode ongeveer gelijk is.⁴⁰ Open source software is qua veiligheid dus geen panacee; ook hiervoor blijven updates nodig om fouten te verhelpen. Het is dus niet onmogelijk om malware te ontwikkelen voor bijvoorbeeld het Linux of MacOS besturingssysteem, maar met een marktaandeel dat veel kleiner is dan Windows zullen de inkomsten voor malware even-redig minder zijn.

Het is aannemelijk dat als het MacOS of Linux besturingssysteem marktaandeel wint, meer malware zal volgen. Massale migraties van een marktleidend softwareproduct naar een alternatief verhogen dus niet de veiligheid, volgens dit argument. De focus van malware zal dan namelijk verschuiven naar de nieuwe marktleider.

Diversiteit is wenselijk

Deze redenering verklaart weliswaar de onbeveiligheid van de huidige monocultuur,

38 'Halloween Document I (Version 1.17), Open Source Software: A (New?) Development Methodology', Raymond, E.S., www.catb.org.

39 Kerckhoffs' principle in 'Secrecy, Security, and Obscurity', www.schneier.com.

40 'Tale of Four Kernels', Spinellis, D. ACM, Germany, 2008, www.spinellis.gr.

maar is tegelijk geen goed argument tegen IT-diversiteit. Het is bijvoorbeeld onwaarschijnlijk dat marktaandeelen in de softwaremarkt zullen omslaan, laat staan snel zullen wijzigen. Het aantal gebruikte applicaties op een platform, lopende investeringen, gesloten of 'semi-open' standaarden, onbekendheid van alternatieven, de benodigde nieuwe kennis voor behoudende gebruikers, gekleurde 'feiten' en de angst voor verandering remmen migraties naar andere software af. Het voordeel van migratie blijft dus sowieso langer bestaan dan deze redenering doet vermoeden.

Stelling 2 – Als organisaties standaardiseren op software introduceren ze een 'single point of failure' dat misbruikt kan worden door malware. De hoogte van dat risico hangt af van het marktaandeel van de gebruikte software.

Ondanks alle goede bedoelingen, zoals het actieplan 'Nederland Open in Verbinding' uit 2007, is Nederland sterk afhankelijk geworden van enkele dominante softwareleveranciers.⁴¹ Open standaarden worden wel breed ondersteund, maar te weinig gebruikt. Van gebruikte software wordt zelden geverifieerd of deze open standaarden correct toepast, zonder deze standaard te 'verrijken' met gesloten technologie. In de praktijk vermindert de afhankelijkheid van dominante softwareleveranciers hierdoor nauwelijks.

Uniformering en diversificatie van software

In de landbouw is al eeuwenlang bekend dat een monocultuur ziektes en plagen aantrekt. Als een gewas in een monocultuur eenmaal is besmet, gaat een groot deel van de oogst verloren omdat de kans dat een besmetting wordt doorgegeven maximaal is. Erop gokken dat schaalvergroting goed blijft gaan, is zeer risicovol gebleken, zeker wanneer de belangen van de hele samenleving op het spel staan.⁴² Daarom verbouwen boeren niet op alle percelen hetzelfde gewas en wisselen ze elke paar jaar per perceel van gewas.

Monocultuur

De huidige IT-monocultuur maakt dat het cyberrisico voor de Nederlandse samenleving maximaal is. De kans is namelijk maximaal dat Nederlandse systemen malware oppikken, omdat voor marktleidende software verreweg de meeste malware circuleert. De impact is eveneens maximaal, omdat een besmetting kan worden doorgegeven aan het merendeel van de systemen. Als een virus een groot aantal systemen kan besmetten, kunnen cascade effecten ontstaan. Omdat er binnen vitale sectoren veel computersystemen zijn die werken met marktleidende software, is dit voor Nederland een reëel risico. Reeds in 1999 zei congreslid Curt Weldon: *'It's not a matter of whether America will have an electronic Pearl Harbor... it's a matter of when'*.



FOTO ANP
In augustus 2012 besmette het Dorifel-virus zo'n drieduizend Windows-systemen bij dertig Nederlandse organisaties

In augustus 2012 besmette het Dorifel-virus zo'n drieduizend Windows-systemen bij dertig Nederlandse organisaties, waaronder veel gemeenten. Het bleek dat alle systemen al (veel) eerder ongemerkt besmet waren met het Citadel-virus, die het Dorifel-virus uitrolde. Als Dorifel niet zo opzichtig de inhoud van programma's en MS-Officebestanden had vercijferd, was de besmet-

41 Ministerie van EZ, 'Nederland Open in Verbinding: een actieplan voor het gebruik van Open Standaarden en Open Source Software in de (semi) publieke sector', november 2007, <http://noiv.nl>.

42 Zie de grote hongersnood van 1845 in Ierland: <http://history1800s.about.com>.

ting waarschijnlijk pas veel later opgemerkt.⁴³ Maar helaas leren ook cybercriminelen van hun fouten.

Een gangbare maatregel om de beschikbaarheid van systemen te verbeteren is het inrichten van back-up voorzieningen. Reservesystemen met dezelfde software zijn echter vatbaar voor dezelfde malware als het operationele systeem en zijn dus ineffectief bij een cyberaanval. Organisaties kunnen nog steeds standaardsoftware kiezen, maar een samenleving wordt kwetsbaar als alle organisaties dezelfde software (blijven) gebruiken. Om binnen Defensie en de vitale sectoren het cyberrisico te spreiden moeten organisaties onderling verschillende software gaan gebruiken (diversificatie).

Stelling 3 – De impact van malware vermindert door software te kiezen:

- met een klein marktaandeel,
- waarvoor fouten en kwetsbaarheden snel gerepareerd worden,
- waarvan de programmacode klein en hoogwaardig is,
- die open standaarden correct gebruikt.

Effecten van diversificatie

De effecten van diversificatie kunnen met een eenvoudig netwerkmodel globaal worden berekend.⁴⁴ Een organisatie die overstapt van het marktleidende product A naar een alternatief product B met een lager marktaandeel, zal daardoor minder geraakt worden door malware. Daarnaast remt diversiteit ook de verspreiding van malware af, aangezien de kans op een 'vruchtbaar contact' vermindert. Hierdoor verbetert de balans tussen besmetting en ont-

smetting en kan malware (veel) minder systemen besmetten. Software diversiteit kan zo malware epidemieën voorkómen.⁴⁵

Organisaties die migreren naar andere software maken éénmalig extra kosten voor opleidingen en conversie. Dat geldt ook als een organisatie bijvoorbeeld wil overstappen naar een volgende versie van Office-software. Hiermee is diversificatie een beveiligingsmaatregel als elke andere: een investering. Het Amerikaanse *Department of Defense* is daarom deels overgestapt op Apple-computers.⁴⁶ Ook het KNMI heeft voor een belangrijk systeem een back-up met een ander besturingssysteem, andere hard- en software en door een andere leverancier gebouwd.⁴⁷

Voor Defensie is relevant dat potentiële aanvallers (veel) moeilijker twee verschillende systemen gelijktijdig uit kunnen schakelen. Tijdens de Koude Oorlog hadden de NAVO-landen een nucleaire *Second Strike Capability*, maar die risicospreiding vergde een strategische voorbereiding en een daarvoor toereikend budget. Met een risicoanalyse kan Defensie vaststellen waar het cyberrisico op deze manier moet worden gespreid.

Niet alle organisaties dezelfde standaardsoftware

Meer standaardiseren op marktleidende software is vergelijkbaar met bezuinigen op brandeuren in gebouwen – terwijl bekend is dat de wijk steeds meer pyromanen aantrekt. Meer diversiteit in standaardsoftware verbetert de veiligheid, omdat het risico van malware wordt gespreid over verschillende producten en de besmettelijkheid van malware wordt vermindert.

Nederland kan de impact van cyberincidenten verminderen als organisaties niet allemaal dezelfde standaardsoftware gebruiken. De impact vermindert het meest als de markt evenwichtig verdeeld is. Als bijvoorbeeld twee producten elk vijftig procent marktaandeel hebben, neemt de *return-on-investment* voor malware met vijftig procent af omdat een malware-programma maar maximaal de helft van de systemen kan

43 'XDocCrypt/Dorifel – Document encrypting and network spreading virus', Fox-IT, 9 augustus 2012, <http://blog.fox-it.com>.

44 'Math on Malware', *ISACA Journal* (3) 2011, www.isaca.org.

45 'Security through Network-wide Diversity Assignment', O'Donnell, A.D., september 2005, <http://idea.library.drexel.edu/bitstream>.

46 'Apples For The Army', Greenberg, A., *Forbes.com*, 21 december 2007, www.forbes.com.

47 Zie: www.knmi.nl.

besmetten. Ook hergebruik van gerichte malware wordt moeilijker als de softwaremarkt meer verdeeld is. Het dwingt cybercriminelen om meer nieuwe malware te ontwikkelen, die per stuk ook nog eens minder opleveren. Diversificatie raakt de internetmaffia dus waar het zeer doet: het reduceert de inkomsten van malware.

Voor softwareleveranciers zal meer diversiteit in de markt naar verwachting het aantal openstaande *Zero-day exploits* per product verminderen en daarmee meer tijd opleveren om kwetsbaarheden in software te repareren. Dit geldt ook voor meer softwarebedrijven in de markt, aangezien die bedrijven de neiging hebben hun kostbare programmacode zoveel mogelijk opnieuw te gebruiken in verschillende producten. Dit versterkt het veiligheidseffect, omdat de periode waarin kwetsbaarheden kunnen worden misbruikt korter wordt. Vanuit het oogpunt van veiligheid is diversificatie dus een maatregel die een voordeel oplevert dat op andere manieren moeilijk te behalen is.

Als de software een klein marktaandeel heeft en kwetsbaarheden snel worden gerepareerd, kan de daarop gerichte malware minder computers infecteren. Als een softwarepakket bovendien een compacte programmacode heeft met een hoge kwaliteit, wordt het voor cybercriminelen moeilijker en dus duurder om malware te maken voor deze software. Dit verlaagt de *Business Case* voor dergelijke malware.

Naar een veiliger cyberdomein

Organisaties die back-upsystemen uitrusten met andere software dan productiesystemen verminderen daarmee het cyberrisico, maar verhogen tegelijkertijd hun beheerskosten. Migreren naar een alternatief besturingssysteem is daarom alleen te overwegen bij vitale systemen. Organisaties kunnen makkelijker overstappen op alternatieve standaardsoftware voor websurfen, Office en e-mail. Dergelijke migraties zijn voor gebruikers relatief laagdrempelig: de meeste softwareproducten bieden dezelfde functionaliteit, alleen de bediening verschilt (zoals een computer met

Windows, een Apple-iPad en een Android-tablet onderling verschillen).

Als de hele organisatie op alternatieve standaardsoftware overstapt, roept dat in eerste instantie weerstand op, bijvoorbeeld omdat gebruikers en beheerders nieuwe kennis moeten opbouwen. Migreren naar andere standaardsoftware kan daarom het beste samenvallen met het uitfasen van oude softwareproducten. Het nadenken over een exit-strategie maakt echter zelden deel uit van het aanschaftraject voor nieuwe software. Veel organisaties onderschatten de impact van softwaremigraties. Als een organisatie niet kan loskomen van het oude standaardproduct, krijgt het nieuwe product vaak de schuld. Alleen met een goede voorbereiding en het gebruik van open standaarden, kunnen organisaties de afhankelijkheid van leveranciers verminderen.

De gemiddelde computergebruiker gebruikt thuis graag dezelfde software als op kantoor. Organisaties die het thuisgebruik van nieuwe standaardproducten mogelijk maken, verhogen daarmee het draagvlak voor de verandering. Bovendien elimineert dit het risico dat thuiswerkers illegale software gebruiken, die vaak geïnfecteerd is met malware.

Het is voor organisaties dus financieel aantrekkelijk om te standaardiseren op gratis software

Maatregelen als diversificatie van software moeten worden gecoördineerd boven het niveau van individuele organisaties. De *European Network and Information Security Agency* (ENISA) bepleit het internationaal oppakken van meerdere lange-termijnmaatregelen tegen cybercrime (zie tabel 4).

Om een goede variatie in softwareproducten te bereiken is het noodzakelijk dat internationaal

Acties en maatregelen	Effect
<ul style="list-style-type: none"> • Harmonisatie van wetten om de samenwerking te verbeteren bij de opsporing en aanhouding van cybercriminelen; isoleren van besmette computers en uitschakelen van malafide servers • Filtering, blokkering en infiltratie van besmette computers • Gestructureerd aanpakken waardeketen van cybercrime • Coördinatie van research om IT kwaliteit, veiligheidskennis en bewustwording te verbeteren 	<p>Betere preventie van infecties met malware</p>
<ul style="list-style-type: none"> • Verbeteren detectie, identificatie en analyse van malware • Ondersteun eigenaren van besmette computers bij de ontsmetting • Harmonisatie van wetten voor het neutraliseren van besmette computers • Coördinatie van acties op malware ontwikkelingen • Coördinatie van research voor een betere beveiliging 	<p>Betere ontsmetting van besmette computers</p>

Tabel 4. Internationale coördinatie van cybersecurity

het marktaandeel van softwareproducten en de hoeveelheid malware per softwareproduct objectief worden bewaakt en gepubliceerd. Momenteel is het marktaandeel en de hoeveelheid malware per softwareproduct moeilijk vast te stellen. Dat komt omdat voor veel onderzoeksrapporten geld wordt gevraagd, de schattingen van marktaandelen sterk uit elkaar kunnen lopen en informatie gekleurd kan zijn.⁴⁸ Voor alle relevante bronnen is informatie over de onderzoekscontext nodig om de statistieken goed te kunnen interpreteren.

Bij gelijke geschiktheid is het wenselijk een standaardproduct te kiezen dat correct werkt met open standaarden, zodat gegevensuitwisseling met andere software beter gegarandeerd is en afhankelijkheid van leveranciers wordt verminderd. Uitgesloten moet worden dat softwareproducten open standaarden 'verrijken' met gesloten technologie. Hierdoor is migratie naar andere producten in de toekomst ook beter mogelijk.

Vanwege de huidige IT-monocultuur is het cyberrisico voor de Nederlandse samenleving maximaal. Het Amerikaanse ministerie van Defensie is daarom deels overgestapt op Apple-computers

Conclusies en aanbevelingen

Door IT breed toe te passen en systemen online te koppelen zijn bedrijfsprocessen veel efficiënter geworden. Om de concurrentie in the *global village* in de toekomst aan te kunnen, zal Nederland steeds meer processen digitaal moeten



⁴⁸ Zie bijvoorbeeld de schattingen van de marktaandelen van Adobe Reader en MS Exchange vs. Lotus Notes.

koppelen. Daardoor zal de afhankelijkheid van ICT-systemen nog meer toenemen. Om informatie te kunnen delen is overigens alleen het gebruik van dezelfde interfacestandaard nodig, het gebruik van dezelfde software is niet vereist. Het internet met zijn open standaarden is daar zelf het beste voorbeeld van.

De netwerksamenleving is echter een tweesnijdend zwaard. Door de uniformering van software, meer online toepassingen, de autonome groei van het internet en de gevolgen van de financiële crisis stijgt het risico op malware-besmettingen. Reguliere beveiligingsmaatregelen zoals firewalls en antivirussoftware zijn steeds slechter opgewassen tegen infecties met malware. Zelfs een optimale beveiliging kan besmettingen met malware niet uitsluiten, zodat elke organisatie een Incident Response Plan moet hebben voorbereid.

Om het risico op aanvallen met cyber te verminderen, kunnen organisaties procedures en beveiligingsregels aanscherpen en medewer-

kers gratis de zakelijke software verstrekken voor thuisgebruik, inclusief beveiligingssoftware. Organisaties die hiervoor geen licentiekosten willen maken, standaardiseren op gratis software. Ook het verminderen van besmette privécomputers door het bevorderen van veiligheidsbewustzijn levert de samenleving als geheel voordeel op.

Open software en IT-diversiteit bevorderen

Elke organisatie kan zelfstandig standaardsoftware kiezen, maar een samenleving wordt kwetsbaar als de meerderheid van de systemen dezelfde software gebruikt. Verschillende onderzoeken hebben al gewaarschuwd tegen de risico's van een (te) uniform IT-landschap, maar de afgelopen jaren waren de veranderingen van de marktaandelen in de softwaremarkt gering.⁴⁹

In tegenstelling tot de *Convention on Biological Diversity*, is het nog ongewoon het gebruik van open standaarden en ICT diversiteit met beleid af te dwingen.⁵⁰ Hoewel iedereen het logisch vindt dat de hardware van vitale systemen dubbel is uitgevoerd, worden back-upsystemen meestal voorzien van dezelfde software. Vasthouden aan marktleidende software die het meest aantrekkelijk is voor cybercriminelen betekent echter (impliciet) instemmen met een hoger risico op cyberaanvallen.

Goede voorbereiding

Aan de andere kant wordt het onacceptabel geacht als een cyberaanval nucleaire systemen, havens, het betalingsverkeer, telecommunicatiesystemen, de drinkwatervoorziening, ziekenhuizen, de energievoorziening of Defensie grootschalig lam legt. Tijdens een cyberaanval kan niet onmiddellijk een vervangend systeem met andere software uit de grond worden gestampt. Om te vermijden dat een cyberaanval een domino-effect van vitale voorzieningen veroorzaakt is een strategische voorbereiding vereist.



FOTO US DEPARTMENT OF DEFENSE

49 ENISA, 'Security Economics and The Internal Market' (hoofdstuk 7), www.enisa.europa.eu. Zie ook: 'Perspective: Massachusetts Assaults Monoculture', Greer, D., CNET News, <http://news.cnet.com>.

50 'Convention on Biological Diversity', www.cbd.int.

Defensie loopt in vredetijd het risico dat met een cyberaanval logistieke en financiële informatiesystemen worden gesaboteerd. In conflict-situaties kunnen gehackte operationele militaire systemen mensenlevens kosten.

De kennis en betrokkenheid van Defensie is nodig om cyberaanvallen op Nederlandse vitale belangen zo moeilijk mogelijk te maken en capaciteit op te bouwen om aanvallen snel te kunnen pareren. Defensie kan daarmee de invulling van haar hoofdtaken en de communicatie daarover verbeteren, zodat realistische verwachtingen ontstaan over wat wel en niet binnen de verantwoordelijkheid van Defensie valt.

Internationale coördinatie

Betere maatregelen, meer deskundigen en internationale coördinatie zijn nodig om het cyberdomein veiliger te maken. Het is belangrijk om het gebruik van open standaarden te bevorderen, om 'single points of failure' door dezelfde software te vermijden. Daarnaast moeten landen hun wetten internationaal harmoniseren, om de waardeketen van cybercrimijnen multinationala aan te kunnen pakken.

Meer research kan de veiligheid van systemen verhogen en de bestrijding van malware verbeteren. Omdat malware steeds meer schade veroorzaakt aan de samenleving moeten alle effectieve tegenmaatregelen worden ingezet. ■



FOTO US DEPARTMENT OF DEFENSE

Een Amerikaanse luchtmacht-generaal houdt een pleidooi voor meer samenwerking en betere internationale coördinatie tijdens een cyberconferentie in Stuttgart

Het kind

Linda Polman

In Port-au-Prince, Haïti, beslissen rechters dezer dagen of ex-dictator Jean-Claude 'Baby Doc' Duvalier terecht moet staan wegens financiële wanpraktijken en mensenrechtenschendingen tijdens zijn presidentschap, dat duurde van 1971 tot 1986. Of de zaak doorgang vindt, hangt af van de overtuigingskracht van vier hoofdgetuigen, ex-gevangenen die de martelingen in Jean-Claude's gevangenis overleefden.

De hoorzittingen halen lang niet elke dag de voorpagina's in Haïti. Vraag het ze en de meeste Haïtianen zeggen 'laat Jean-Claude nou maar, hij was nog maar een kind'. Jean-Claude was pas 19 toen hij het presidentschap van zijn vader erfde.

Jean-Claude was in alles zijn vaders tegenpool. Waar de zoon altijd voorrang gaf aan plezier boven zaken, was de vader, François 'Papa Doc' Duvalier, 24 uur per dag in touw om land en volk in wreedheid en terreur ondergedompeld te houden. Papa Doc moet het product geweest zijn van een liefdesrelatie tussen Hitler, Caligula en de Taliban. Vaak stond wit schuim hem letterlijk op de lippen en hij putte groot genot uit het persoonlijk doodmartelen van mensen die hem tegenstonden; dat was in principe iedere Haïtiaan die slim of sterk en daardoor bedreigend was. Honderdduizenden werden door de dictator het land uitgejaagd, tienduizenden verdwenen in gevangnissen en massagraven. Leger en politie vertrouwde hij ook voor geen cent. Liever liet hij zich dienen door zijn privé-militie, de *Tonton Macoutes*, genoemd naar de boeman die in de Haïtiaanse folkloré 's nachts rondsluipert om stoute kinderen in zijn rieten zak te proppen. Over de Macoutes-structuur had Papa Doc goed nagedacht. Hij ronselde zijn leden in de laagste sociale klassen. Macoutes waren bijna zonder uitzondering analfabeet, zwart en tot in hun oorlellen rancuneus ten opzichte van Haïti's lichtgekleurde zakelijke, intellectuele en militaire elite. Het lidmaatschap van de Tonton Macoutes gaf de ongeletterden het recht om iedereen, met name de rijken, te beroven, bedreigen en vermoorden. Duizenden meldden zich aan voor het begeerlijke baantje,

hele families legden hutje bij mutje om vader of zoon aan een lidmaatschapskaart te helpen en zo de familie hun enige kans op geld en macht te geven.

Met het aantreden van de zoon veranderde het objectief. Jean-Claude, die nog met autootjes speelde, was te lui en ook te dom om totale controle na te streven. Van zijn moeder móest hij rechten en sociologie studeren, dus kwamen professoren van de universiteit hem thuis in het paleis onderwijzen. Na een kwartiertje luisteren viel hij steevast in diepe slaap. Vaak deden de professoren alsof ze dat niet in de gaten hadden. Ze gaven les aan de slapende gestalte, terwijl een secretaresse aantekeningen maakte.

Toen de onderzoeksrechter hem dezer dagen vroeg of het waar is dat er destijds standrechtelijke executies plaatsvonden, antwoordde Jean-Claude: 'Dat weet ik niet. Ik bemoeide me niet met dat soort zaken'. Hetgeen waar is. Het interesseerde hem allemaal geen biet. Jean-Claude richtte zijn leven adembenemend simpel in. Hij schreef op een cheque de naam van een of andere institutie, daaronder zijn eigen naam en het woord cash en dan verzilverde hij de boel. Zo plukte hij miljoenen van de staatsloterij, het ministerie van Financiën, het elektriciteitsbedrijf, de nationale bank en de belastingdienst.

In vergelijking met de vader was de zoon een verademing, zeggen Haïtianen. Zijn luiheid had grote voordelen. Vluchtelingen kwamen terug naar huis, internationale ontwikkelingshulp kwam weer op gang, buitenlandse investeerders openden assemblagefabrieken in ruil voor belastingvoordeeltjes en toeristen vierden vakantie in een splinternieuwe *Club Med*. En laten we wel wezen: wie geen Macoute was geweest, had wel geprobeerd het te worden. Driehonderdduizend leden telde de organisatie aan het eind van Jean-Claude's presidentschap. Een paar miljoen familieleden van Macoutes profiteerden ervan. Het heeft echt zijn redenen wel dat er nu geen meutes buiten de rechtszaal staan om het hoofd van de voormalige dictator te eisen. ■

Wapens voor Syrië?

Dr. M.F.J. Houben – luitenant-kolonel der Mariniers*

Wanneer en hoe steun je vrijheidsstrijders? Dit is een vraag die in de internationale politiek regelmatig terugkeert en die iedere keer weer voor hoofdbrekens en verdeeldheid zorgt. Het basisgegeven is duidelijk en onomstreden: een volk komt in opstand tegen een misdadig regime. Het regime gebruikt vervolgens alle machtsmiddelen om de opstand neer te slaan. Vervolgens ontstaat een 'vrijheidsleger' dat de gewapende strijd met de regeringstroepen aangaat. De strijd die volgt is doorgaans langdurig en meedogenloos. Het moment dat er zoiets als een vrijheidsleger is en we (enigszins) zicht op het verloop van de strijd hebben, is het moment waarop de internationale gemeenschap zich serieus gaat bezinnen op praktische opties om de vrijheidsstrijders te steunen.

Binnen de internationale gemeenschap bestaat geen consensus rond wapenleveranties aan Syrië

Syrië is inmiddels een triest toonbeeld van de ellende, complexiteit en uitzichtloosheid van een moderne vrijheidsstrijd en de situatie laat zich zeer vereenvoudigd als volgt schetsen. Het Syrische volk is verwickeld in een bloedige vrijheidsstrijd teneinde zich te ontdoen van

het regime-Assad. Het Syrische verzet is georganiseerd rondom de *Syrian Opposition Coalition* (SOC) en het *Free Syrian Army* (FSA), de gewapende arm van de SOC. Het FSA is in een ongelijke (asymmetrische) strijd verwickeld met het regeringsleger: een geregeld leger tegen een onduidelijke, nauwelijks georganiseerde en slecht uitgeruste groep strijders die je wellicht als een 'ongeregelde militia' zou kunnen omschrijven. En hoewel het FSA de door hen bezette buitenwijken van Damascus als *liberated areas* omschrijft, liggen ze dagelijks onder vuur van artilleriebeschietingen en luchtaanvallen. En het volk lijdt.

Om aan deze ongelijke strijd een einde te maken heeft de Syrische oppositie de internationale gemeenschap verzocht om steun in de vorm van wapenleveranties. Meer precies: om geleide antitankwapens en luchtdoelraketten. Deze wapens zouden het FSA in staat moeten stellen om succesvol op te treden tegen het regeringsleger. Dit lijkt een logisch en voor de hand liggend verzoek en je zou aannemen dat daar dan ook een logisch en voor de hand liggend antwoord vanuit de internationale gemeenschap op zou (moeten) volgen. Ik vraag mij echter af of het wel zo logisch en voor de hand liggend is om Syrië van wapens te voorzien.

Op dit punt wil ik enkele *caveats* maken: ten eerste is dit geval tot op zekere hoogte hypothetisch – zo zou het kunnen gaan; ten tweede beschik ik, als geïnformeerd krantenlezer, niet over alle informatie en ten slotte is de uiteindelijke beslissing een politieke. Ik zal mij derhalve beperken tot de militair-technische overwegingen.

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

Er bestaat binnen de internationale gemeenschap geen consensus ten aanzien van dit Syrische verzoek. Sommige experts vinden het verstandiger om militaire adviseurs in plaats van wapens ter ondersteuning van het FSA naar Syrië te sturen. Het Vrije Syrische Leger wil daar echter niets van weten, zij wensen geen vreemde militairen op Syrische bodem; ‘Geef ons de wapens die we nodig hebben en wij, leden van het Vrije Syrische leger, zullen een einde aan het regime maken’, zo luidt het devies.

Mijn twijfel begon bij de volgende overweging. Geleide antitankwapens zijn gecompliceerde systemen, misschien niet in de praktische zin van ‘gemakkelijk in het gebruik’, maar wel qua onderhoud en zeker wat betreft de inzet onder gevechtssomstandigheden. De *operator* moet getraind zijn om een dergelijk wapensysteem te gebruiken. Sterker, hij moet goed getraind zijn om het wapensysteem goed in te kunnen zetten en het maximale tactische effect te realiseren. De training voor de operator van een dergelijk geavanceerd systeem duurt enkele maanden en omvat training in simulators en in het veld. Het is onduidelijk of een dergelijk trainingspakket deel uitmaakt van het ondersteuningspakket dat de Syrische vrijheidsstrijders nodig hebben, of er tijd voor training is en of het Vrije Syrische Leger dat accepteert.

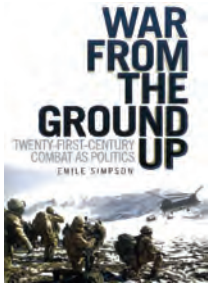
De tweede overweging betreft de aard van het optreden van het Vrije Syrische Leger. Hoewel het te vroeg is voor een definitieve analyse van het conflict in Syrië, kunnen drie fasen worden onderscheiden. In de eerste fase zagen we het onvermogen van het conventioneel getrainde regeringsleger om met een *guerilla insurgency* om te gaan (en dus het relatieve succes van het FSA). Daarna kwam een fase waarin het regeringsleger actief de strategische punten ging verdedigen tegen mogelijke aanvallen door het FSA. In de derde, huidige fase, hebben de strijdende partijen relatief vaste posities ingenomen of zijn ze die aan het innemen. Dit is het mogelijke begin van een ‘stellingenstrijd’ waarin het Vrije Syrische Leger steeds meer gedwongen wordt om positie in te nemen en om terrein(delen) te verdedigen. Stel nu dat het FSA de beschikking krijgt over dergelijke ‘zware’ geleide antitankwapens en luchtdoel-

raketten, dan wordt dat FSA mogelijk nog langzamer en nog meer terreingebonden.

Met andere woorden: dergelijke wapensystemen maken het optreden van het FSA conventioneeler. Het directe gevolg is dat het FSA zich daarmee – geheel ongewild en onbedoeld – transformeert tot een (conventionele) tegenstander waar het regeringsleger wél mee om weet te gaan. Het relatieve succes van het FSA lag juist in die schimmigheid en onvoorspelbaarheid, niet in het wapenarsenaal.

Antitankwapens en luchtdoelraketten zouden het FSA kunnen transformeren tot een conventionele tegenstander

Mocht de internationale gemeenschap besluiten om dergelijke wapensystemen aan het FSA te geven, met de bedoeling hen te versterken in de strijd tegen het regime, dan kan het (onbedoelde) gevolg zijn dat de opstandelingen juist minder succesvol worden in hun optreden omdat ze langzamer, conventioneeler en meer terreingebonden gaan opereren. In plaats van het FSA te ondersteunen zou een dergelijke goedbedoelde actie de ondergang kunnen inluiden. De strijd in Syrië illustreert daarmee niet alleen de angels en voetklemmen waarvoor de internationale gemeenschap zich gesteld ziet om een legitieme strijd te kunnen ondersteunen, maar illustreert mogelijk ook de volle omvang van de *unintended consequences* van (politieke) beslissingen op operationeel niveau. ■



War From the Ground Up

Twenty-First-Century Combat as Politics

Door Emile Simpson

Londen (Hurst & Co.) 2012

256 blz.

ISBN 9781849042550

€ 23,-

War From the Ground Up is een stimulerend, filosoferend boek over de 21ste-eeuwse interactie tussen de inzet van het militaire instrument en veiligheidspolitiek in moderne liberale democratieën. Dit is gecompliceerd omdat, zoals auteur Emile Simpson schrijft, ‘The control of political space is as important, if not more important, than controlling physical space’ (blz. 6). De functie van het militaire instrument verandert op alle niveaus. Simpson, kapitein bij de Britse *Royal Gurkha Rifles* en *visiting fellow* aan Oxford University, constateert: ‘The military dimension of war is pierced by political considerations at the tactical level’. Simpson heeft ruime operationele ervaring ‘aan de basis’ in vooral Afghanistan, die hij weet te combineren met zijn krijgswetenschappelijke kennis. In het boek krijgt de constatering aldus *body*, waarbij veel doet denken aan het *three-block war* model zoals generaal Charles Krulak van het *United States Marine Corps* dat beeldend beschreef in de jaren ’90.

Het belang van duurzame vrede

War From the Ground Up bevestigt dat oorlogen niet meer op het slagveld gewonnen worden; het winnen van een duurzame vrede is de crux. Oorlog schept niet langer condities voor een afgedwongen politieke oplossing, maar is een instrument om een fundament te leggen waarop politieke oplossingen gebouwd kunnen worden. Het gaat om *armed politics*: ‘an interpretive mechanism that gives force political utility’ (blz. 30). Zeer uiteenlopende doelgroepen moeten overtuigd worden van het nut, het belang en de noodzaak van de inzet van het militaire instrument en het vinden van een breed gedragen politieke oplossing van een vaak lang lopend conflict. Gevolg hiervan is dat, ‘If one uses war as an instrument to achieve a political outcome, one must align actions with an understanding of how the recipient will interpret them’ (blz. 31). Militairen moeten daarom de ‘political kaleidoscopic dynamics of the conflicts’ (blz. 45) doorgronden, waarbij Bosnië, Irak en Afghanistan voorbeelden zijn. Simpson pleit hiermee indirect voor sociaalwetenschappelijk onderlegde officieren.

Een probleem bij de uitvoering van een hedendaagse veiligheids-

strategie – in een doorgaans zeer complexe en interdependente maatschappelijke omgeving – is dat het vanuit militair perspectief noodzakelijk is te integreren met anderzootige organisaties. Bovendien is continue en directe interactie met politici gedurende inzet onvermijdelijk. De complexiteit wordt verder vergroot doordat tegenwoordige oorlogen in (politiek gefragmenteerde) coalitieverbanden gevoerd worden met gevolgen voor het vormen en ondersteunen van eenduidige intenties. Rupert Smith merkte eerder al op dat ‘The glue that holds a coalition together is a common enemy, not a common desired political outcome’.¹ Het Clausewitziaanse adagium dat oorlog de voortzetting van de politiek met andere middelen is, dient op een geëvolueerde manier geïnterpreteerd te worden. De tijd van vertrouwen in louter wapentuig ligt achter ons. De voorbeelden die Simpson hiertoe gebruikt zijn exemplarisch en hij werkt ze in korte *casestudies* uit.

Uitdagingen

In de hedendaagse politiek-militaire arena draait het om de context waarin de intentie van het actieve gebruik van het militaire instrument vorm krijgt: ‘In contemporary conflict physical destruction tends to matter less to a conflict’s outcome than how those actions are perceived [...] The outcome is defined against several audiences who are not the enemy’ (blz. 187). Simpson pleit voor intensief gebruik van strategische communicatie en een *strategic narrative* om uiteenlopende publieke opinies (inclusief de eigen) te bespelen, eenheid te smeden en het denken en

¹ Rupert Smith, *The Utility of Force. The Art of War in the Modern World* (Londen, Allen Lane, 2005) 302.

doen in termen van *effects-based operations*. Zijn boodschap is dat 'War has moved towards becoming a direct extension of political activity' (blz. 232). De politieke, strategische en operationele realiteit dient zich hieraan aan te passen, waartoe Simpson gaandeweg het boek een aantal suggesties doet.

Simpsons *War From the Ground Up* is een treffend voorbeeld van *officer-scholarship* en de uitdagingen die

ontstaan voor politici, beleidsmakers en militairen hoe om te gaan met militair-operationele inzet in een globaliserende, *inter-connected* wereld: 'War today is [...] transformed by the information revolution, which forces liberal powers to reconsider strategic thought in relation to their use of armed force' (blz. 89). Simpson neemt de lezer gemakkelijk mee in zijn denkwijze over de moderne krijg en de complexe politiek-militaire omgeving

waarin deze plaatsvindt. Hij concludeert dat deze verwevenheden en interdependenties gevolgen hebben voor de hedendaagse doctrines, maar dat die nog onvoldoende geëvolueerd en geïmplementeerd zijn. *War From the Ground Up* geeft een forse aanzet voor moderne doctrinevorming en conceptueel denken: verplichte kost voor strategen, beleidsmakers en commandanten.

Dr. drs. A.J.E. Wagemaker MA,
luitenant-kolonel der Mariniers

AANKONDIGING

Algemene ledenvergadering KVBK en lezing Rob Bertholee

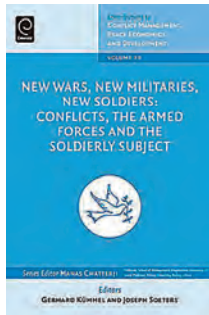
Op 21 mei 2013 organiseert de KVBK de jaarlijkse Algemene Ledenvergadering, gevolgd door een lezing van Rob Bertholee, directeur AIVD en luitenant-generaal buiten dienst van de Koninklijke Landmacht.

Leden van de KVBK zijn welkom vanaf 16.30 uur. De ledenvergadering begint om 17.00 uur en duurt tot uiterlijk 17.30 uur. Agendapunten kunnen worden aangeleverd bij de secretaris: secretaris@kvbk.nl.

De lezing van Rob Bertholee staat open voor alle geïnteresseerden en begint om 17.30 uur. U kunt zich voor deze lezing opgeven via secretaris@kvbk.nl.

De ledenvergadering en de lezing vinden plaats in de nieuwe persruimte van het Plein Kalvermarkt Complex in Den Haag. Meer details volgen in de april-editie van de *Militaire Spectator* en via twitter (@KVBK1) en facebook ([facebook.com/KVBKNederland](https://www.facebook.com/KVBKNederland)).





New Wars, New Militaries, New Soldiers? Conflicts, the Armed Forces and the Soldierly Subject

Door Gerhard Kummel en Joseph Soeters (red.)
Bingley (Emerald Publishing Group) 2012
251 blz.
ISBN 9781780526386
€ 110,-

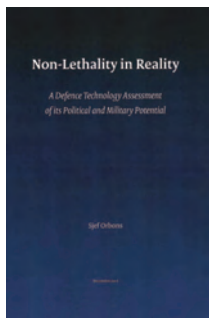
In deze bundel, die deel uitmaakt van de reeks *Contributions to Conflict Management, Peace Economics and Development*, kijken sociologen naar de strijdkrachten en conflictbeheersing. Zij focussen daarbij op drie recente ontwikkelingen: de veranderingen in het type conflict van interstatelijk naar irregulier, de economische neergang die de defensiebegrotingen onder druk zet en de herstructurering van dienstplichtlegers naar organisaties van vrijwilligers en professionals. 'Nieuwe' conflicten, waaronder ook de bestrijding van terrorisme, vergen van defensieorganisaties en militaire eenheden een andere manier van plannen en organiseren. Volgens de auteurs is de druk op defensieorganisaties toegenomen, waarbij het draait om de vraag welk maatschappelijk doel schaarse financiële middelen moeten hebben.



Moed moet

Verslagen van Nederlandse veteranen, van
Nederlands-Indië tot Uruzgan
Door David Vriesendorp en Fred Hoogeland
Houten (Het Spectrum) 2012
176 blz.
ISBN 9789000316632
€ 19,99

Moed moet is een verzameling verhalen van Nederlandse veteranen die na de Tweede Wereldoorlog zijn ingezet in diverse oorlogs- en crisisgebieden in de wereld. De veteranen, zowel actief dienenden als militairen die de dienst verlaten hebben, zijn openhartig over morele en ethische dilemma's en over leiderschap. Ze beschrijven hun motieven om bij de krijgsmacht te gaan en geven een oordeel over de kwaliteit van de training die zij kregen voordat zij werden ingezet. Het voorwoord in het boek is geschreven door oorlogsverslaggever Peter te Velde, terwijl de auteurs verder spraken met onder meer Peter van Uhm, Marco Kroon, Patrick Cammaert, Giovanni Hakkenberg en John Titahena.



Non-Lethality in Reality

A Defence Technology Assessment of its Political
and Military Potential
Door Sjef Orbons
Breda/Amsterdam (NLDA/proefschrift Universiteit
van Amsterdam) 2013
166 blz.
ISBN 9789088920530

Het gebruik van *non-lethal weapons* (NLW's, niet-dodelijke wapens zoals traangas en plastic kogels) bij het winnen van *hearts and minds* van de bevolking is alleen effectief als de bevolking een politiek perspectief wordt geboden, zo concludeert Sjef Orbons in zijn proefschrift. Orbons onderzocht in hoeverre de operationele omstandigheden de taakgerichte prestaties en effecten van NLW's beïnvloeden. Zonder een aanvaardbaar politiek perspectief worden NLW's toenemend gezien als onderdrukkingsmiddel. De samenwerking tussen militaire eenheden die NLW's gebruiken en de groepen die onder controle gehouden worden, leidt tot een dalende effectiviteit van de wapens. Uiteindelijk worden NLW's zelfs ongeschikt voor de beheersingstaak.



Van Zadar tot Dubrovnik

Het relaas van een vredesmissie
Door H. van de Beek
Dronten, 2011
268 blz.
€ 27,-
verkrijgbaar via auteur:
h.vandebeek-dronten@solcon.nl

Hans van de Beek maakte eind 1991-begin 1992 als marine-officier deel uit van de EG Monitor Missie die moest toezien op de naleving van een bestand in Joegoslavië. De missie, de eerste in haar soort die de EG opzette, bestond uit diplomaten en militairen, die probeerden te bemiddelen bij de moeizame en bijna eindeloze onderhandelingen tussen de strijdende partijen. Van de Beek, gestationeerd in Dalmatië, schetst de gebeurtenissen tegen de achtergrond van het Joegoslavië-beleid van 'Brussel', waarbij hij onder meer ingaat op het uitwisselen van gevangenen, bedreigingen, militair geweld, leugens en bedrog en de belegering van kazernes van het Joegoslavische leger.

Met dank aan bibliotheek NLDA

SUMMARIES

Th.B.F.M. Brinkel and J.E. Noll – The ‘Belfast Flag Issue’ and the Vulnerable Peace in Northern Ireland

On Christmas Eve 2012 the city council of Belfast decided that the Union Jack should no longer be hoisted 365 days a year, but only on special designated days. This decision triggered an outburst of disturbances. The authors discuss why Northern Ireland is an important case to research reconciliation and reconstruction in order to understand similar problems in other countries or regions. This case also

has relevance for those who reflect on peace operations and the concept of a comprehensive approach to bring safety, justice, a democratic order and social and economic development as elements of post-conflict restructuring. Finally, Northern Ireland provided experiences with resistance, counterinsurgency, terrorism and counter-terrorism that may lead to other lessons.

J. Müller and R. de Winter – Allied Force as a new Feat of Arms for the Royal Netherlands Air Force

In 1999 NATO's air operation Allied Force was to force the Serbian president Milosevic to leave Kosovo. In June, three months after the start of the operation, two Dutch F-16s were confronted by MiGs and anti-aircraft weapons. Both pilots were decorated later. In 2010 the Commander of the Air Force proposed the minister of Defence to award the entire Air Force with a banner for the Kosovo campaign. The authors shortly describe this campaign and clarify in detail the process

that finally led to the approval of the banner request. In this process the analysis of the operational context and the application of five criteria determined the outcome that the Air Force rightfully deserved this award, the first in kind for the Air Force since 1965.

H.J. van der Molen – Cyber Security: Relevant Trends for Defence

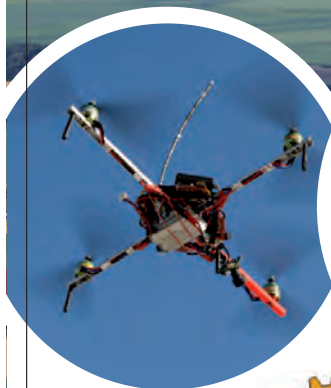
Since June 2012 Dutch Defence has a Cyber Strategy. It underlines the importance of the cyber domain for the execution of operations and for the safeguard of broader national interests. The author focuses on the risks that Defence and other users of information systems face. Those risks require specific knowledge and insight in the risks and impact of cyber incidents or cyber attacks is needed for protection and reaction. The author reflects on trends

concerning cyber incidents and the economic model behind cyber attacks. He describes why the reduction of the risk of incidents is problematic, under which circumstances these risks are high and the effect that may result from protective measures. The author addresses the organizational level as well as IT-professionals and the individual user of information systems.

2013 Kooy Symposium



UNMANNED AERIAL SYSTEMS



KIVI NIRIA

TNO innovation
for life

PROGRAMMA

11.00 - 12.00	Setting the scene
12.00 - 13.00	Lunch, workshops en tentoonstelling
13.00 - 14.30	Beleid en visie
14.30 - 15.30	Pauze
15.30 - 15.45	Uitreiking Prof. Kooy prijs
15.45 - 17.00	Excellente technologieën
17.00 - 17.15	Afsluiting
17.15 - 18.00	Borrel
18.00 - 19.00	Nasimaaltijd

ONDERWERPEN

- Politieke aspecten
- Ervaring inzet en gebruik
- UAS aanvullend of vervangend
- Gevolgen personeel en inzet
- Internationale samenwerking
- Technische uitdagingen
- Nederlandse technologie

LOCATIE + TIJD

Woensdag 3 April 2013

Aanvang : 11.00 uur
Einde : 19.00 uur

Marine-etablisement
Amsterdam