



# MILITAIRE SPECTATOR



Beiroet 1983 - New York 2001

**Thema**  
**'Inlichtingen en veiligheid'**



#### UITGAVE

Koninklijke Vereniging ter  
Beoefening van de Krijgswetenschap  
www.kvbk.nl

#### Secretariaat KVBK

(Ledenadministratie, PR, secretaris  
en penningmeester)  
MPC 41A  
Postbus 9012 6710 HC Ede  
info@kvbk.nl

#### Secretaris:

luitenant-kolonel I.M. de Jong  
Telefoon: (0318) 68 32 30

#### HOOFDREDACTEUR

**brigade-generaal prof. J.M.J. Bosch**

Instituut Defensie Leergangen  
MPC 58B  
Postbus 20701, 2500 ES Den Haag  
Telefoon (015) 284 42 58  
of (076) 527 32 09  
Fax (015) 284 47 21

#### REDACTIE

kolonel drs. P.J.E.J. van den Aker  
kolonel KLu J.F.W. van Angeren  
drs. P.H. Kamphuis  
luitenant-kolonel mr. M.Th.J. Messer-  
schmidt  
commodore KLu F.H. Meulman  
kolonel drs. J. Terpstra  
kolonel ir. R.G. Tieskens  
commodore KLu J.C. Willemse

#### BUREAUREDACTIE

mw. drs. A. Kool  
p/a hoofdredacteur  
Telefoon (015) 284 47 20  
Fax (015) 284 47 21  
a.kool@mindef.nl

#### ADVERTENTIES

CET Reclame & Publiciteit  
Telefoon (0497) 53 15 31

#### ABONNEMENTEN

binnenland: € 20 (f 44,07)  
studenten: € 12 (f 27,55)  
buitenland: € 25 (f 55,09)

#### DRUK

Drukkerij Giethoorn Ten Brink  
Vormgeving: TS Media  
ISSN 0026-3869

#### NADRUK VERBODEN

Foto-omslag: abc-press



# MILITAIRE SPECTATOR

## INLEIDING

- 558** Editoriaal:  
Inlichtingen en veiligheid
- 560** Mededelingen
- 561** Inleiding door drs. W.J. Kuijken:  
De coördinatie van de Nederlandse inlichtingen- en veiligheids-  
diensten in verleden, heden en toekomst

## DE NATIONALE DIMENSIE

- 564** dr. D. Engelen: De Nederlandse inlichtingen- en veiligheidsdiensten  
in de 20ste eeuw
- 577** J.A. van Reijn: De Militaire Inlichtingendienst, vandaag en morgen
- 587** S.J. van Hulst: Op weg naar een Algemene Inlichtingen- en  
Veiligheidsdienst

## DE INTERNATIONALE DIMENSIE

- 593** F.E. van Kappen: Strategische inlichtingen en de Verenigde Naties
- 598** drs. R. Theunens: Intelligence en vredesoperaties
- 604** J.R. Karssing: De NAVO en inlichtingen
- 613** H.A.J. Bokhoven: Inlichtingen in de Europese Unie

## RISICO'S EN DREIGINGEN

- 616** drs. E.S.M. Akerboom: Terrorisme aan het begin van de 21ste eeuw
- 621** drs. S. Stienstra: Biologische wapens
- 628** drs. J.A. van der Louw: Information Operations: informatie als doel,  
middel én wapen
- 636** ir. H.A.M. Luijff: Bitbreuken verwacht; zijn wij erop voorbereid?

## DIVERSEN

- 643** drs. B.M. de Jong: De Russische diensten en hun verleden
- 654** Overzicht inlichtingen- en veiligheidsdiensten NAVO-partners
- 655** Samenvattingen / Summaries

## INLICHTINGEN EN VEILIGHEID

Dit themanummer ontstond niet omdat de wereld op 11 september jongstleden met de aanslagen op het *World Trade Center* en het *Pentagon* werd geconfronteerd. Reeds maanden geleden besloot de redactie daartoe. Bijna alle opgenomen artikelen kwamen vóór die dag tot stand. De redactie had een aantal overwegingen om de schijnwerpers indringend op het inlichtingendomein te richten.

Allereerst het gegeven dat inlichtingenanalyses het fundament van politiek-militaire (en politionele) besluitvorming heten te zijn. Met het verdwijnen van de Oost-West-tegenstelling maakte de door de Koude Oorlog getekende dreiging plaats voor andere veiligheidsrisico's. Risico's voor zowel de complexe westerse samenleving, als voor operationeel ingezette eenheden. De schending tussen interne en externe veiligheid is vervaagd en de vraag rijst hoe het inlichtingendomein op deze veranderingen heeft gereageerd of zou moeten reageren.

Daarnaast de vele gezichten van 'inlichtingen en veiligheid', zeker als het wordt gekoppeld aan diensten, structuren en processen. Vele gezichten óók, omdat diensten zich veelal niet alleen richten op het verzamelen van inlichtingen, maar ook op het tegengaan van dit soort activiteiten (contra-inlichtingen), of breder het bewerkstelligen van veiligheid of het beschermen van vooral de nationale rechtsorde. Vele gezichten verder, omdat sprake is van verschillende dimensies: de politieke, de militaire en de civiele, alsmede van verschillende niveaus: het strategische, het operationele en het tactische. Ten

slotte, maar zeker niet op de laatste plaats, vormde de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten' aanleiding voor dit themanummer.

Mede door de opheffing van de Inlichtingendienst Buitenland (IDB) ontstond behoefte aan een nieuwe wettelijke grondslag. De nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten ligt nu bij de Eerste Kamer. Er ontstaan een Algemene- en een Militaire Inlichtingen- en Veiligheidsdienst (AIVD en MIVD). De wet regelt tot in detail de taken, de bevoegdheden, de transparantie en het toezicht, alsmede het toetsingskader voor bijzondere activiteiten. In de komende periode zullen de diensten hun bedrijfsprocessen op de nieuwe wet moeten afstemmen. Met name de offensieve taak in het buitenland, waaronder de inzet van 'agenten', zal om afstemming en coördinatie vragen.

De ratio voor twee diensten is duidelijk. Ze is ook herkenbaar in vele landen. De AIVD richt zich op de (inter)nationale rechtsorde; de MIVD op de ondersteuning van de minister van Defensie en de strijdkrachten, met name bij besluiten over inzet. Tijdens een inzet vormt de MIVD één van de verzamelorganen voor het ingezette multinationale verband. Zij steunt derhalve niet alleen de minister maar ook de chef defensiestaf, of deze nu 'opperbevelhebber' wordt of niet.

De redactie treedt met dit nummer in de voetsporen van haar voorgangers die vanaf 1914 ruimte boden voor de pennevruchten van H.A.C. Fabius, de grondlegger van de militaire inlichtingendienst, gs III. Deze dienst zou de vader c.q. grootvader worden van alle latere Nederlandse inlichtingen- en veiligheidsdiensten.

In dit nummer wordt vanuit drie optieken naar het thema gekeken. Vanuit de nationale optiek komt de geschiedenis van de Nederlandse inlichtingendiensten, de taak, organisatie en werkwijze van de Militaire Inlichtingendienst (MID), de Binnenlandse Veiligheidsdienst (BVD) nu en morgen, alsmede de coördinatie tussen de diensten aan de orde. Vanuit de internationale optiek gaat de aandacht uit naar de vraag hoe de Verenigde Naties, de NAVO en de Europese Unie inhoud geven aan het verwerven, verwerken, verspreiden en gebruiken van inlichtingen en omgaan met de veiligheidsdimensie. De ervaringen op

<sup>1</sup> Eerste Kamer, vergaderjaar 2000-2001, 25 877, nr. 337.

inlichtingengebied bij de uitvoering van vredesoperaties komen afzonderlijk aan bod. Een derde optiek vormt mogelijke risico's en dreigingen. Wat valt er te zeggen over terrorisme in het algemeen en over biologische wapens, over *information operations* en over de kwetsbaarheid van de Nederlandse informatie-infrastructuur in het bijzonder? Ten slotte besteden wij aandacht aan een specifiek aspect van de inlichtingenwereld: de worsteling tussen openheid en geheimhouding (waarbij memoires van KGB-medewerkers als voorbeeld worden gebruikt). Een overzicht van diensten in diverse landen illustreert de complexiteit. Kortom, in dit themanummer gaat het om 'inlichtingen en veiligheid' in brede zin.

De gebeurtenissen van 11 september maken wel dat het onderwerp terrorisme uiterst actueel is: dit komt ook op de omslag tot uiting. De aanslag op het WTC was meer dan een terreurdaad tegen de Verenigde Staten. Het was een aanslag op de internationale rechtsorde: weerloze burgers uit talrijke landen waren het doelwit. Anderen – net zo weerloos – werden in vliegtuigen die als bom fungeerden de dood in gejaagd. Nog nooit vielen er zoveel slachtoffers in één terroristische operatie. Het was overigens niet de eerste keer dat de bevolking doelwit is; het zal vermoedelijk ook niet de laatste keer zijn. Terreur is in de ogen van sommigen een middel om een politiek doel te bewerkstelligen. De terroristen, variërend van ETA tot IRA, van de 'Rode Brigades' tot het netwerk van Osama bin Laden, kennen niet hetzelfde geloof, dezelfde nationaliteit of dezelfde overtuiging. Gemeenschappelijke kenmerken vormen haat en het gehanteerde middel: terreur.

Ook krijgsmachten kunnen overigens doelwit van een terroristische actie zijn. Op de omslag daarom ook een foto uit 1983. Op 23 oktober van dat jaar rijdt een terrorist in een vrachtauto gevuld met explosieven het gebouw van het Eerste Bataljon van de Amerikaanse Mariniers in Beiroet binnen. Deze actie veroorzaakt 241 doden. Tweeëndertig gewonden overlijden later. Bijna tegelijkertijd wordt in dezelfde stad net zo'n actie uitgevoerd tegen het Franse militaire hoofdkwartier. Hierbij vallen 58 doden en vijftien gewonden.

De aanslagen in de Verenigde Staten eisen nu vooral vooruitzien en doelgerichte samenwerking.

king. Ooit komt het moment dat achterom kan worden gezien. Dan komt de vraag op wat de Amerikaanse en bevriende diensten hebben gedaan of nagelaten. Vast staat dat zij de gebeurtenissen niet wisten te voorkomen. Ook dat is niet nieuw. Keer op keer werden landen, werd de wereld verrast; was wat er gebeurde niet voorzien. De val van de Muur, de implosie van DDR, het Warschau-Pact en de USSR zijn illustratief. Hoeveel moeilijker is het om zicht te houden op de heimelijke activiteiten van tien, honderd of zelfs duizend fanatici die bereid zijn terreur uit te oefenen, terwijl zij de mogelijkheden van techniek en wetenschap daarbij benutten en de kwetsbaarheden van onze moderne samenleving goed kennen?

Moeilijk of niet, de inlichtingen- en veiligheidsdiensten zullen nieuwe wegen moeten vinden om veiligheidsrisico's te onderkennen en tijdig actie te ondernemen. Sir Michael Alexander, voorzitter van het *Royal United Services Institute for Defence Studies* voorspelde in 1999 dat de inlichtingenfunctie zou veranderen: *'it will, in particular, become much more 'joint' i.e. it is going to require ever closer co-operation between the police and other internal security organs; the armed forces; overseas intelligence gathering agencies, overt and covert; agencies specialising in photographic, signals and computer analysis; banks etc. It is also bound to involve much more co-operation between states and within international organisations.'*<sup>2</sup>

De internationale gemeenschap zal wel moeten. Op 11 september werd duidelijk hoe 'klein' de wereld is geworden; hoe 'alles' met 'alles' samenhangt. De moderne landen vormen één financiële wereld; één wereld van handel en verkeer en één mediawereld. Alle landen delen één milieu. Elk incident raakt het totale systeem en kan enorme gevolgen hebben. Dreigingen en risico's, maatregelen en oplossingen hebben niets meer met landsgrenzen van doen. Meer en meer blijkt dat de nationale soevereiniteit en het nationaal belang als begrip aan het verouderen zijn. Dit besef en politieke wilskracht zou moeten verzekeren dat samenwerking echt inhoud krijgt.

De conclusie luidt dat de wereld verre van perfect is. Daarom zijn er inlichtingen- en veiligheidsdiensten nodig. Zij dienen bij te dragen aan vrijheid van handelen en de bescherming van de rechtsorde. Dit themanummer wil aan dit besef bijdragen.

<sup>2</sup> RUSI-journal, October 1999, p. 5

# Mededelingen

## Netherlands Intelligence Studies Association (NISA)

Dit speciale nummer van de Militaire Spectator over inlichtingen- en veiligheidsdiensten is tot stand gekomen in samenwerking met de *Netherlands Intelligence Studies Association* (NISA). De NISA, in het Nederlands geheten Stichting Inlichtingenstudies Nederland (SISN), is in 1991 opgericht en stelt zich tot doel de studie van inlichtingen- en veiligheidsdiensten te bevorderen. Zij organiseert daartoe o.a. lezingen en van tijd tot tijd een congres over een met inlichtingen- en veiligheidsdiensten verband houdend onderwerp.

De NISA heeft in de herfst van 1999 in Amsterdam een internationaal congres georganiseerd over de betekenis van *Signals Intelligence* (SIGINT) tijdens de Koude Oorlog. Een uitgewerkte versie van de lezingen van het congres plus enkele toevoegingen, zal eerdaags in boekvorm verschijnen bij Frank Cass onder de titel *Secrets of Signals Intelligence during the Cold War* (Matthew M. Aid & Cees Wiebes, editors). Dit boek zal tevens als apart nummer verschijnen van het tijdschrift *Intelligence and National Security*. Er zijn hoofdstukken opgenomen over: 'NSA and the Cold War', 'GCHQ and SIGINT in the Cold War' en verder over SIGINT in Canada, de Bondsrepubliek Duitsland, Frankrijk, Scandinavië en Nederland tijdens de Koude Oorlog.

Sinds kort heeft de NISA ook een eigen website:

<http://www.nisa-intelligence.nl/> NISA, Postbus 18210 1001 ZC Amsterdam



### Komende nummer:

In MS12 onder meer:

kolonel J.R. Mulder:  
Inlichtingen bij HQ 1 (GE/NL) Corps;

luitenant-kolonel E.A.O. Onderdelinden:  
Verbindingsinlichtingen;

J.K. McDonald:  
Intelligence and Strategic Surprise;

drs. P.E. van Loo:  
De inzet van 306 Squadron boven voormalig  
Joegoslavië 1993-1999.

# De coördinatie van de Nederlandse inlichtingen- en veiligheidsdiensten in verleden, heden en toekomst

drs. W.J. Kuijken\*

Voor u ligt een unieke *Militaire Spectator*. Voor het eerst in de geschiedenis van dit eerbiedwaardige tijdschrift is een volledig nummer gewijd aan het onderwerp *Intelligence*. Iets dat in het nog niet zo lange verleden ondenkbaar zou zijn geweest. Het is mij een eer en genoegen als coördinator van de inlichtingen- en veiligheidsdiensten een bijdrage te kunnen leveren aan dit themanummer. Ik ben ervan overtuigd dat de artikelen, geschreven door zowel *intelligence-professionals* als wetenschappers, uw aandacht meer dan waard zijn. Zelf zal ik in onderstaand artikel trachten u enig inzicht te verschaffen in een boeiend onderdeel van mijn werkzaamheden bij het ministerie van Algemene Zaken: het coördineren van de werkzaamheden van de twee inlichtingen- en veiligheidsdiensten die Nederland rijk is, de Militaire Inlichtingendienst en de Binnenlandse Veiligheidsdienst.

## Geschiedenis professionele I&V-diensten Nederland

Inlichtingenwerk, informatie verzamelen, spioneren zoals sommigen het noemen, is zo oud als de mensheid. Altijd is er behoefte geweest aan informatie, niet alleen op militair maar ook op politiek en economisch gebied. En met het vak van het verzamelen van dergelijke informatie ont-

stond uiteraard een tegenbeweging, die van het voorkomen daarvan. De professionalisering van beide métiers liep van land tot land uiteen. De geschiedenis van de professionele I&V-diensten in Nederland is nog een vrij jonge. Direct voor de Eerste Wereldoorlog werd de onder het ministerie van Oorlog ressorterende derde sectie van de Generale Staf (GS III) opgericht. Echter, zoals beschreven in *De Militaire Inlichtingendiensten*, de weerslag van een door dr. Dick Engelen verricht institutioneel onderzoek,<sup>1</sup> lieten de prestaties van die dienst in de periode kort voor het uitbreken van de Tweede Wereldoorlog te wensen over. Hoe dan ook, het uitbreken van de Tweede Wereldoorlog gevolgd door de bezetting van ons land door de Duitsers, drukte de naar Engeland gevluchte Nederlandse regering pijnlijk op het ontbreken van voldoende goede informatie. De regering in Londen besloot daarom tot de oprichting van de Centrale Inlichtingendienst. Na de oorlog werd vervolgens als eerste de Buitenlandse Inlichtingendienst (BID) opgericht, kort daarna gevolgd door de oprichting van de Centrale Veiligheidsdienst, de voorloper van de Binnenlandse Veiligheidsdienst (BVD). Verder beschikte het ministerie van Oorlog over een inlichtingenapparaat dat was ondergebracht bij de Generale Staf, alsmede een Marine Inlichtingendienst (MARID).

Al spoedig constateerde mr. C.L.W. Fock, toenmalig raadadviseur van de minister-president, dat de nog jonge I&V-diensten langs elkaar heen werkten en dat coördinatie tussen de diensten noodzakelijk was. In 1948 leidde

dit tot de oprichting van de Commissie van Coördinatie (CvC) die – formeel – onder voorzitterschap stond van de minister-president. Na de oprichtingsvergadering werd de voorzittershamer in de praktijk gevoerd door de staatssecretaris van het ministerie van Oorlog. Fock, die intussen secretaris-generaal van het ministerie van Algemene Zaken geworden was, werd secretaris. Het coördineren tussen de diensten was kennelijk geen eenvoudige taak. Na een enthousiast begin en een periode van frequente vergaderingen, betrokken de I&V-diensten de Commissie van Coördinatie steeds minder bij hun interne en onderlinge problemen. Vanaf medio '52 kwam de Commissie zelfs niet meer bijeen. Dit was voor Fock de aanleiding om bij de minister-president de opheffing van de CvC en de aanstelling van een coördinator te bepleiten.

## CVIN en miciv

Dit leidde ertoe dat op 13 februari 1956 vice-admiraal buiten dienst F.J. Kist werd benoemd tot de eerste Nederlandse coördinator van de inlichtingen- en veiligheidsdiensten. Vastgelegd werd dat de coördinator ressorteerde onder de minister-president, in diens hoedanigheid van minister van Algemene Zaken. Kist nam al spoedig het initiatief tot de oprichting van het Comité Verenigde Inlichtingendiensten Nederland (CVIN), dat in mei 1957 door de minister-president ingesteld werd. Twintig jaar later, in 1976, besloot de Minister-raad, op voorstel van coördinator F.E. Kruimink (eveneens een vice-admiraal b.d.), tot de oprichting van de

\* De auteur is secretaris-generaal van het ministerie van Algemene Zaken, coördinator van de inlichtingen- en veiligheidsdiensten.

<sup>1</sup> Rijksarchiefdienst, *De militaire inlichtingendiensten, een institutioneel onderzoek naar het handelen van de overheid op het gebied van militaire inlichtingendiensten, 1945-1999* (PIVOT-rapport nummer 61).



**Coördinatie gebeurt op het Binnenhof** (Bron: foto Chris van Etten © RVP)

Ministeriële Commissie voor de Inlichtingen- en Veiligheidsdiensten (MICIV).

Ten slotte werd in 1991 de secretaris-generaal van het ministerie van Algemene Zaken, mr. R.J. Hoekstra, de eerste niet-militaire coördinator. De aldus vormgegeven coördinatiestructuur bestaat nog steeds. De MICIV met de minister-president als voorzitter bepaalt het algemeen beleid betreffende de inlichtingen- en veiligheidsdiensten en is belast met de coördinatie van de diensten. Het CVIN bereidt het overleg van de MICIV voor en treedt op als voorportaal van die commissie. De coördinator van de inlichtingen- en veiligheidsdiensten is niet langer afkomstig uit defensiekringen maar uit de civiele overheid. Hij is voorzitter van het CVIN en is op i&v-gebied de belangrijkste adviseur van de minister-president.

Hoe verloopt die coördinatie in de praktijk. Feitelijk vindt die plaats in de vergaderingen van het CVIN, die in principe maandelijks worden gehouden. In het CVIN hebben de directeur

van de MID, het hoofd van de BVD, de (plaatsvervangend) directeur-generaal Politieke Zaken van het ministerie van Buitenlandse Zaken en de directeur-generaal Rechtshandhaving van het ministerie van Justitie, onder voorzitterschap van de coördinator, zitting. Indien er zaken aan de orde komen die andere ministeries regarderen, worden ook vertegenwoordigers daarvan uitgenodigd. In de praktijk zijn dit vaak Verkeer en Waterstaat, vertegenwoordigd door de directeur-generaal Telecommunicatie en Post en Economische Zaken, vertegenwoordigd door de plaatsvervangend secretaris-generaal. Soms neemt ook de loco-secretaris-generaal van Financiën deel. Alle deelnemers aan het overleg in het CVIN kunnen onderwerpen agenderen die het werk van MID en/of BVD aangaan. Uiteraard overlegt de coördinator ook regelmatig bilateraal met de leiding van de diensten. Waar mogelijk zal de coördinator streven naar samenwerking tussen beide diensten en trachten te komen tot afstemming van beider

activiteiten. Dit kan uitmonden in gezamenlijk opgestelde rapportages ten behoeve van de MICIV.

Afstemming en samenwerking tussen de diensten wordt bewerkstelligd in het CVIN zelf, maar ook in door het CVIN ingestelde werk- of adviesgroepen, die soms een permanent en soms een ad hoc-karakter hebben. Het wetsontwerp voor de nieuwe 'Wet op de Inlichtingen- en Veiligheidsdiensten' (WIV) is zo totstandgekomen, maar ook de regeringsnotitie over het grootschalig afluisteren van moderne telecommunicatie (deze laatste naar aanleiding van de discussie in het Europees Parlement over het zogenaamde Echelon-systeem).

De MICIV wordt bijeengeroepen indien besluitvorming op ministerieel niveau gewenst is. De besluiten van de MICIV worden vervolgens altijd aan de orde gesteld in de op de MICIV volgende vergadering van de Minister-raad. Aldus ontstaat een door het voltallige kabinet gedragen besluitvorming.

## Wet op de Inlichtingen- en Veiligheidsdiensten

De nieuwe WIV is reeds ter sprake gebracht. De Tweede Kamer heeft deze wet inmiddels aanvaard en verwacht mag worden dat ook de Eerste Kamer zich nog dit jaar uitsprekt. Indien ook de Eerste Kamer tot een positief oordeel komt, dan zullen de diensten in 2002 op grond van de bepalingen van de nieuwe WIV werken. Deze wet ademt de geest van deze tijd. Het is een omvangrijke wet geworden waarin uitvoerig de taken en bevoegdheden van de diensten en van de coördinator zijn omschreven. De wet voldoet aan alle eisen van openheid en transparantie en is in lijn met de opvattingen zoals die in Europa heersen.

De wet markeert het grote verschil tussen I&V-diensten van vroeger en nu. De 'oude' diensten werkten zoveel als mogelijk in het geheim, op basis van een wet die zich kenmerkte door beknoptheid. Sporadisch haalden de diensten de publiciteit en ook de politiek bemoeide zich nauwelijks met hun werk (wellicht met uitzondering van de BVD, wiens activiteiten traditioneel meer aan de burger raakten).

De diensten van nu staan midden in de maatschappij. Hun activiteiten raken direct en indirect aan de belangen van burgers, bedrijfsleven en onderdelen van de overheid. Diezelfde maatschappij is zich in de afgelopen jaren ook veel meer dan voorheen voor de I&V-diensten gaan interesseren. De deelname van ministeries als Verkeer en Waterstaat en Economische Zaken aan de beraadslagingen van CVIN en MICIV, illustreert deze ontwikkeling.

### MIVD en AIVD

Sedert de opheffing van de Inlichtingendienst Buitenland (IDB) per 1 januari 1994, telt Nederland nog twee diensten, de MID en de BVD, na inwerkingtreding van de nieuwe WIV respectievelijk Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en Algemene Inlichtingen- en Veiligheidsdienst (AIVD) geheten. Dat lijkt wei-

nig, maar beide diensten verenigen het totale scala aan inlichtingenwerk in zich. In de MIVD (MID) zijn de eerder zelfstandige landmacht-, lucht- en marine inlichtingendiensten verenigd, alsmede de organisaties die zich op het gebied van de verbindingsinlichtingen bewegen. Bij de AIVD (BVD) is inmiddels het Nationaal Bureau voor Verbindingsbeveiliging ondergebracht en wordt de inlichtingentaak buitenland toegevoegd, een taak die de MID op militair gebied reeds had. Die toevoeging maakt dat, vanaf de inwerkingtreding van de nieuwe WIV, de BVD, dan AIVD, zich ook formeel tot de *foreign intelligence community* mag rekenen.

### Intensievere bemoeienis minister-president en coördinator

De rode draad in de geschiedenis van de coördinatie van de I&V-diensten is de rol van de minister-president, minister van Algemene Zaken. Ook in de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten is die rol gehandhaafd en zelfs enigszins aangezet waar het gaat om de inlichtingentaak buitenland van de diensten. De minister-president zal, in overeenstemming met de ministers van Defensie en Binnenlandse Zaken en Koninkrijksrelaties, bepalen of een dienst een (inlichtingen)opdracht in het buitenland moet gaan uitvoeren. Deze rol vergt een intensievere bemoeienis van de minister-president en de coördinator. De voorbereiding van dergelijke besluiten zal immers in het CVIN, in samenspraak met behoeftestellers en uitvoerende diensten, worden voorbereid. En de coördinator is vervolgens verantwoordelijk voor de advisering van de minister-president. Met het oog hierop is bij het ministerie van Algemene Zaken de positie van de coördinator verzaagd. Door de benoeming van een plaatsvervangend coördinator, tevens plaatsvervangend secretaris-generaal van Algemene Zaken, wordt bewerkstelligd dat de eventuele afwezigheid van de coördinator niet tot stagnatie van besluitvorming hoeft te leiden. De coördina-

tor kan rekenen op de ondersteuning van de adviseur I&V-beleid en de raadadviseur Buitenland. Overwogen wordt om daarnaast met liaisons van AIVD en MIVD bij Algemene Zaken te gaan werken.

### Toekomst Nederlandse 'Intelligence'

De inwerkingtreding van de nieuwe WIV zal een nieuwe episode van de Nederlandse *Intelligence* markeren. Duidelijk is dat de diensten zich veel meer dan voorheen mogen verheugen in een brede belangstelling van zowel publiek als politiek. Openheid en transparantie waar dat kán, en een goede verantwoording zijn daarin de reeds eerder genoemde trefwoorden. Dat de diensten met deze veranderende rol kunnen omgaan, blijkt onder meer uit de openbare jaarverslagen die zowel MID als BVD uitbrengen. In de WIV is bepaald dat ook een Commissie van Toezicht zal worden benoemd. Deze commissie, waarvan de leden worden benoemd op voordracht van de Tweede Kamer, houdt, onafhankelijk van regering en parlement, toezicht op de rechtmatigheid van de taakuitoefening van de diensten én van de coördinator. Ook adviseert de commissie de betrokken ministers over het onderzoeken en beoordelen van klachten.

De nieuwe WIV biedt zowel aan de diensten als aan de coördinator nieuwe bevoegdheden, kansen, uitdagingen en verplichtingen. Mijn doel is erop gericht om tezamen met de directeur van de MID en het hoofd van de BVD ervoor te zorgen dat de diensten hun werk kunnen verrichten in de geest van deze tijd. Transparant waar mogelijk, gesloten waar noodzakelijk, met oog voor de belangen van burgers, bedrijfsleven en overheid en rekening houdend met de eisen van de moderne democratische rechtsstaat.

Zoals in het editoriaal gesteld: onze wereld is verre van vredig. De inlichtingen- en veiligheidsdiensten worden met grote uitdagingen geconfronteerd. Het thema van dit nummer is uiterst actueel.



# De Nederlandse inlichtingen- en veiligheidsdiensten in de 20ste eeuw

## Een overzicht

dr. D. Engelen\*

### Inleiding

Zoals zoveel innovaties was de eerste Nederlandse inlichtingendienst een militaire aangelegenheid. Van een innovatie kon zeker gesproken worden toen in 1913 formeel de derde sectie van de Generale Staf werd opgericht, in de ook toen al heersende cultuur van afkortingen GS III genaamd. De innovatie bestond vooral daarin dat nu voor het eerst de chef van de Generale Staf de beschikking kreeg over een gespecialiseerd en permanent orgaan dat men met enige welwillendheid inlichtingendienst zou kunnen noemen. Vóór die tijd had de krijgsmacht bij voorkomende gelegenheden wel (tactische) inlichtingen ingewonnen, zoals tijdens de Tiendaagse Veldtocht in 1830, maar van een echte inlichtingendienst was geen sprake geweest. Na de definitieve afscheiding van België had onze krijgsmacht in Europa geen andere taak meer gehad dan het handhaven van de neutraliteit, een taak die naar de toenmalige inzichten kennelijk verricht kon worden zonder een geïnstitutionaliseerde inlichtingendienst. Pas toen aan het

begin van de twintigste eeuw de voor- tekenen van een militair conflict allengs dreigender werden stelde de chef van de Generale Staf, luitenant-generaal C.J. Sniijders, de inlichtingensectie GS III in, daartoe gestimuleerd door de toenmalige minister van Oorlog en voormalig beroepsofficier H. Colijn.

GS III zou de vader c.q. grootvader worden van alle inlichtingen- en veiligheidsdiensten die er sindsdien in ons land zijn geweest. Zoals ook elders, bijvoorbeeld in het Verenigd Koninkrijk, het geval was, waren het de grote conflicten van de twintigste eeuw die de ontwikkeling van die diensten op beslissende manier hebben beïnvloed: de Eerste Wereldoorlog en de nasleep daarvan, vervolgens de Tweede Wereldoorlog en – in het verlengde daarvan – ten slotte de Koude Oorlog.

### GS III

Sinds de Tiendaagse Veldtocht had het Nederlandse leger geen militaire operaties meer uitgevoerd. Het hand-

haven van de neutraliteit vormde de hoeksteen van de Nederlandse buitenlandse politiek. Dat betekende weliswaar niet dat de legerleiding zich afsloot voor wat er in de omringende boze wereld gebeurde, maar van een systematische verkenning van de politieke en militaire *Umwelt* was toch geen sprake. Daarmee werd pas een begin gemaakt na de Frans-Duitse oorlog van 1870, toen het Algemeen Staffbureau van de Generale Staf gegevens ging verzamelen over de krijgsmacht en defensieorganisatie van de Europese landen. Deze gegevens werden bewaard in een dossier 'Vreemde legers en afschriften', dat zijn naam dankte aan het feit dat het werd gevoed uit twee bronnen: rapportage van de Buitenlandse Dienst en uittreksels ('afschrijven') van buitenlandse militaire tijdschriften.

Naarmate het duidelijk werd dat het grote buurland Duitsland op expansie uit was, met name in Afrika, namen aan het begin van de twintigste eeuw de internationale spanningen toe. Er ontstond, ook bij de Nederlandse legerleiding, een groeiende behoefte aan inlichtingen over de politiek-militaire *intentions* en militaire *capabilities* van de grote mogendheden, in het bijzonder van het Duitse keizerrijk. In juni 1912 werd de kapitein der artillerie W.J.C. Schuurman gedetacheerd bij de Generale Staf waar hij op basis van open bronnen politiek-militaire overzichten samenstelde. Aan het eind van dat jaar werd hij in die functie opgevolgd door de kapitein der infanterie H.K. Hardenberg, die

\* De auteur, sinds 1966 bij de Binnenlandse Veiligheidsdienst werkzaam, is vanaf 1990 de bedrijfshistoricus van de BVD. In 1995 promoveerde hij op de *Geschiedenis van de Binnenlandse Veiligheidsdienst*. Hij publiceerde onder meer PIVOT-rapporten over de Inlichtingendienst Buitenland en over de Militaire Inlichtingendienst. Van het laatste verscheen tevens een bewerking in boekvorm onder de titel *De Militaire Inlichtingendienst 1914-2000*. Recent schreef hij een PIVOT-rap-

port over de BVD 1945-2000. In opdracht van de minister van Binnenlandse Zaken bereidt hij een studie voor over de BVD in de Koude Oorlog.

PIVOT is een uitvloeisel van de nieuwe Archiefwet en staat voor Project Invoering Verkorte Overbrengingstermijn, dat beoogt overheidsarchieven na dertig jaar (in plaats van vijftig jaar) over te brengen naar de Rijksarchiefdienst.

Schuurmans pionierswerk voortzette en uitbreidde als hoofd en enig personeelslid van wat het Studiebureau Vreemde Legers ging heten.

Een stroom van soms zeer gedetailleerde vragen, hem voorgelegd door de chef van de Generale Staf en afkomstig van minister Colijn, maakte dat Hardenberg de hulp moest inroepen van zijn collega's bij de Generale Staf. Zo werd hij het middelpunt van een netwerk van specialisten die ieder op hun eigen terrein de ontwikkelingen in het buitenland probeerden te volgen. Met hun hulp stelde Hardenberg informatiemappen samen over zaken als bewapening, organisatie en mobilisatievoorbereiding, waardoor het beantwoorden van Colijns vragen werd vergemakkelijkt.

Hardenberg op zijn beurt werd eind 1913 opgevolgd door de eerste-luitenant der huzaren H.A.C. Fabius die gezien kan worden als de eigenlijke grondlegger van de militaire inlichtingendienst. Anders dan zijn voorgangers wachtte hij niet af welke vragen hem voorgelegd zouden worden. Op eigen initiatief stelde hij maandelijks een 'Militair-politiek overzicht' samen dat vanaf juni 1914 werd afgedrukt in de *Militaire Spectator*. Eveneens in de *Militaire Spectator* verschenen van Fabius' hand van tijd tot tijd 'Korte mededelingen omtrent militaire zaken in verschillende landen' die van uitsluitend militair-technische aard waren. Dat het Studiebureau Vreemde Legers op 25 juni 1914 formeel werd omgezet in de derde sectie van de Generale Staf hield een erkenning in van Fabius' kwaliteiten en werkzaamheden, al zal de gespannen internationale toestand in de zomer van 1914 er niet geheel vreemd aan zijn geweest. Fabius werd het eerste hoofd van GS III, maar personeel kreeg hij niet. Dat zou echter snel veranderen.

### De Eerste Wereldoorlog

De in augustus 1914 uitgebroken Europese oorlog stelde niet alleen



**H.A.C. Fabius: grondlegger van de militaire inlichtingendienst**

hogere, maar ook nieuwe eisen aan Fabius. Hij moest de opperbevelhebber en via hem de regering – een enkele keer zelfs de koningin persoonlijk – op de hoogte houden van de militaire ontwikkelingen buiten de landsgrenzen. Bovendien – en dat was een nieuwe taak – moest hij ervoor zorgen dat de inlichtingendiensten van de oorlogvoerende landen in Nederland niet ongestoord hun gang konden gaan. De eerste zorg daarbij was niet zozeer de bescherming van de eigen politieke en militaire geheimen, als wel het waken over de handhaving van de neutraliteit. De redenering was dat men het alle partijen even moeilijk moest maken, om het verwijt te voorkomen dat Nederland partij koos – en partij kiezen zou wel eens als een *casus belli* opgevat kunnen worden. Voor zijn dubbele taak had Fabius dus dringend versterking nodig. Die kreeg hij al in de loop van augustus in de persoon van C.A. van Woelderen, een wegens invaliditeit vroegtijdig gepensioneerd officier, die aan hem werd toegevoegd als naaste medewerker en plaatsvervanger. GS III breidde zich vervolgens snel

uit; de sectie telde aan het eind van de oorlog vijftig personeelsleden onder wie twaalf officieren.

Toch betekende dit sterk gestegen personeelsbestand niet, dat GS III het werk alleen af kon. Met name op het gebied van het contra-inlichtingenwerk kreeg de sectie ondersteuning. Allereerst van de kant van het Wapen der Koninklijke Marechaussee, dat een tiental onderofficieren ter beschikking stelde voor het doen van gerichte onderzoeken, en al spoedig ook van de kant van de politiekorpsen van de grote steden. Rotterdam liep daarbij voorop. Dat was geen wonder, gezien de strategische positie van de Maasstad ten aanzien van het Duitse achterland. Juist hier loerde het gevaar dat een te tolerante houding tegenover bijvoorbeeld Duitsland, Engelse protesten zou uitlokken en omgekeerd. Vandaar dat de Rotterdamse korpschef, een voormalig marineofficier, het hoofd van zijn rivierpolitie de opdracht had gegeven de activiteiten van de oorlogvoerende partijen in de Rotterdamse haven zorgvuldig in de gaten te houden. Daardoor vormde de inlichtingendienst van de Rotterdamse politie en het feitelijk hoofd daarvan, de chef van de rivierpolitie François van 't Sant, een belangrijke informatiebron voor GS III. Ook na het vertrek van Van 't Sant naar Utrecht, waar hij met steun van GS III tot hoofdcommissaris van politie werd benoemd, bleef de inlichtingendienst van de Rotterdamse politie voor Fabius en zijn staf van groot belang. Zozeer zelfs dat Rotterdamse politieambtenaren die onderzoeken deden voor GS III, uit de geheime kas van de sectie een speciale toelage kregen.

Ook politiediensten uit andere steden werden in de loop van de oorlog ingeschakeld bij het contra-inlichtingenwerk van GS III. Dat gold voor Den Haag dat met zijn ambassades en consulaten een natuurlijke habitat vormde voor een veelheid van inlichtingendiensten. Dat gold ook voor Amsterdam, waar de korpschef aan Fabius beloofde dat hij hem zijn han-

digste rechercheur ter beschikking zou stellen. Dat bleek de inspecteur van politie K.H. Broekhoff te zijn die een natuurlijke aanleg voor het (contra-)inlichtingenwerk aan de dag legde. Hij zou zich tijdens de oorlog, maar ook gedurende het gehele interbellum, een steunpilaar van GS III tonen.

Na Rotterdam, Amsterdam, Den Haag en Utrecht, werden in 1917 nog onder meer de politiekorpsen van Vlissingen en Velsen in het relatienetwerk van Fabius opgenomen. Waarschijnlijk gebeurde dat vooral met het oog op de observatie van scheepsbewegingen. Tekenend voor de behoedzaamheid en omzichtigheid waarmee Fabius te werk ging was zijn verzoek aan Broekhoff – die inmiddels Fabius' vertrouwen geheel had gewonnen – om na te gaan of de korpschef van Velsen wel betrouwbaar was.

Zo was de militaire inlichtingendienst – want zo mogen we GS III inmiddels toch wel noemen – van een eenmansbedrijf uitgegroeid tot een organisatie die aan het eind van de Eerste Wereldoorlog ongeveer vijftig man telde, met bovendien een relatienetwerk dat er zijn mocht. Vooral dat laatste zou uitstekend van pas komen toen in november 1918 uit onverwachte hoek een nieuwe uitdaging zich aandiende: de (naar het even leek) acute dreiging van een revolutie.

### **Dreigende revolutie**

Het einde van de Eerste Wereldoorlog betekende niet dat GS III nu weer tot zijn vooroorlogse sterkte teruggebracht kon worden. Integendeel. Juist de beëindiging van de oorlogshandelingen had katalyserend gewerkt op de aspiraties en activiteiten van wat toen revolutionaire bewegingen heetten: eerst hadden de Bolsjewiki in het tsaristische Rusland de macht overgenomen en het land uit de oorlog teruggetrokken; na de wapenstilstand in november 1918 hadden de sociaal-democraten in Duitsland het keizer-

rijk ten grave gedragen en de republiek uitgeroepen. In Nederland had de SDP de bolsjewistische greep naar de macht met enthousiasme begroet. De orthodox-marxistische Sociaal Democratische Partij was in 1909 afgesplitst van de te reformistisch bevonden Sociaal-democratische Arbeiderspartij (SDAP). In november 1918 doopte de SDP zich in navolging van de partij van Lenin om in Communistische Partij in Nederland, in het spraakgebruik weldra Communistische Partij Holland (CPH) genoemd. Het was dan ook vooral van de kant van de CPH dat GS III op basis van met name de berichtgeving van de Amsterdamse politie, revolutionaire actie vreesde.

Tot verrassing van velen en zeker van de regering, was het echter niet de revolutionaire SDP maar de reformistische SDAP die in november 1918 op het punt leek te staan de macht in Nederland over te nemen. Het werd overigens al snel duidelijk dat niet de SDAP als geheel, maar alleen partijleider P.J. Troelstra en enkele gelijkgestemden, gedurende enkele dagen serieus hadden gedacht dat de Nederlandse bourgeoisie vrijwillig haar politieke macht in handen van de socialisten zou leggen. Als Troelstra's 'revolutie die niet doorging' iets duidelijk maakte was het wel, dat ondanks de slechte sociaal-economische omstandigheden waarvan vooral de arbeiders de gevolgen ondervonden, een radicale omwenteling in Nederland geen enkele kans maakte. W.H. Vliegen, een van Troelstra's meest uitgesproken critici in eigen SDAP-kring, zei het zo:

*Een revolutie in een democratisch geregeerd land is een dwaasheid. Ik heb niet vijftig jaar gevochten voor het algemeen kiesrecht, om het enkele maanden na zijn invoering weer af te schaffen.*

Desondanks werd Troelstra's beoordelingsfout nog lang gebruikt als argument om de SDAP uit het regeerkasteel te houden. Pas in 1939 kreeg deze partij regeringsverantwoorde-

lijkheid met twee ministers in het kabinet-De Geer.

Troelstra's onjuiste beoordeling van de politieke situatie had tot gevolg, dat de 'anti-rode' sentimenten in de samenleving versterkt werden. Een symptoom daarvan waren de weliswaar geregisseerde, maar niettemin massale manifestaties van aanhanke-lijkheid aan vaderland, koningshuis en regering. Daarbij had men weinig oog voor het onderscheid tussen de revolutionaire SDP en de in wezen brave SDAP. De door H. Colijn, op dat moment directeur van de Bataafse Petroleum Maatschappij, en anderen georganiseerde Bijzondere Vrijwillige Landstorm en de plaatselijke Burgerwachten, waren gericht tegen zowel de CPH van David Wijnkoop als de SDAP van Troelstra.

Ook de leiding van GS III dacht langs die lijnen. De dienst had in die spannende novemberdagen als vanzelfsprekend taken op het gebied van de binnenlandse veiligheid op zich genomen, en beschouwde zowel de SDAP als de CPH als organisaties die stevig in de gaten gehouden moesten worden.

### **Het interbellum**

Na de gebeurtenissen van november 1918 streefde Fabius er aanvankelijk naar dat GS III, behalve een militaire inlichtingen- en contra-inlichtingendienst, ook een volwaardige binnenlandse veiligheidsdienst zou worden. Ook op dat gebied zou de sectie eigen netwerken moeten hebben van informanten en vertrouwenspersonen in binnen- en buitenland. Broekhoff en Van 't Sant, de meest uitgesproken vertegenwoordigers van het politieke inlichtingenwerk bij de politie, hadden over die plannen van Fabius zo hun twijfels. Broekhoff stelde indringend de vraag aan de orde, of de Generale Staf nu wel de meest aangewezen instantie was om binnenlandse politieke stromingen te volgen en te bestuderen. Er volgden nog enkele overlegondes tussen Fabius, de chef

van de Generale Staf, W.F. Pop, en de minister van Binnenlandse Zaken, Ch.J.M. Ruys de Beerenbrouck. Het resultaat daarvan was uiteindelijk dat Pop met een nota kwam waarin hij de grondslagen uiteenzette voor een nieuw te vormen dienst. Die dienst, die hij centrale inlichtingendienst noemde, zou de regering op tijd moeten waarschuwen voor 'revolutionaire woelingen en propaganda'.

De nota-Pop stelde dat de beoogde centrale inlichtingendienst onder de politieke verantwoordelijkheid zou moeten vallen van de minister van Binnenlandse Zaken. De dienst zou moeten kunnen rekenen op de medewerking van de plaatselijke politiediensten, van de Koninklijke Marechaussee, van wat heette 'burgerlijke vertrouwenspersonen' ('informanten') zouden we nu zeggen) en ten slotte van de militaire inlichtingendienst.

Wie nu had gedacht dat Pop met de centrale inlichtingendienst een burgerlijke, althans niet-militaire dienst op het oog had, te vergelijken met de huidige BVD, kwam bedrogen uit. Pop pleitte er namelijk voor die dienst onder te brengen bij de Generale Staf. Zijn belangrijkste argument daarvoor was, dat hij al een dergelijke dienst onder zich had, namelijk GS III. Bovendien zou op die manier het bestaan van de dienst voor de openbaarheid verborgen blijven, wat lastige vragen vanuit het parlement zou voorkomen. Ook voor zichzelf zag Pop een rol weggelegd: de chef van de Generale Staf zou de verantwoordelijkheid moeten krijgen voor de distributie van de door de nieuwe dienst verzamelde inlichtingen. Als afnemers daarvan zag Pop de regering, in het bijzonder de minister van Binnenlandse Zaken, en in voorkomende gevallen plaatselijke autoriteiten als burgemeesters en korpschefs.

Pops plan kwam dus neer op een constructie waarbij de chef van de Generale Staf de hoogste ambtelijke verantwoordelijkheid zou dragen voor zowel de militaire dienst GS III als - met een andere pet - de civiele

centrale inlichtingendienst. Had hij zijn militaire pet op, dan viel hij onder de minister van Oorlog als politiek verantwoordelijke; had hij de andere pet op dan viel hij onder de minister van Binnenlandse Zaken.

Met als uitgangspunt de nota-Pop werd de Ministerraad het op 27 oktober 1919 eens over de bovenstaande constructie. Minister van Oorlog G.A.A. Alting van Geusau werkte vervolgens de details wat verder uit. In een nota aan Pop zette hij nog eens de puntjes op de i: de Generale Staf zou uitsluitend verantwoordelijk zijn voor de militaire inlichtingendienst. Die werd in twee delen gesplitst. Een deel, GS IIIA, kreeg als taak het verzamelen van inlichtingen over vreemde legers, dus het eigenlijke inlichtingenwerk. Daarnaast kwam er een onderdeel GS IIIB, dat tot taak kreeg het inwinnen van gegevens over 'denkbeelden en stromingen onder officieren, onderofficieren en minderen in het leger' - een militaire veiligheidsdienst dus.

Uitdrukkelijk schreef Alting van Geusau voor, dat de Generale Staf zich had te onthouden van 'het werken ten dienste van de binnenlandse veiligheid'. Die uitspraak liet op zichzelf aan duidelijkheid niets te wensen over, maar werd nogal gerelativeerd door de opmerking dat dit niet de samenwerking uitsloot met 'een bureau dat onder een ander departement ressorteert' - daarmee doelend op de centrale inlichtingendienst onder Binnenlandse Zaken. Ook zou de minister er geen bezwaar tegen hebben wanneer laatstgenoemde dienst zou worden gehuisvest 'in een der lokalen in gebruik bij de generale staf'. Als maar duidelijk was dat de politieke verantwoordelijkheid voor die dienst berustte bij zijn collega van Binnenlandse Zaken, en niet bij hem.

Zo was, in elk geval op papier, vastgelegd dat GS IIIB en de Centrale Inlichtingendienst (CI) twee totaal verschillende diensten waren, vallend onder twee verschillende ministers. In de praktijk echter vormden GS IIIB en

CI één geheel. Dat had vooral te maken met de uiterst schriële manier waarop de minister van Binnenlandse Zaken bijdroeg aan de financiering en bestaafing van de CI. Oorlog leverde daardoor verreweg de grootste financiële bijdrage, ook aan de CI. Doordat Binnenlandse Zaken bovendien ook niet of nauwelijks personeel beschikbaar stelde, ondanks gedane beloften, ontstond al snel de situatie dat GS IIIB en CI wat personeel betreft samenvielen, zeker in de leidende posities.

Nadat de cavalierist Fabius na de reorganisatie van GS III naar zijn oorspronkelijke onderdeel was teruggeplaatst, nam zijn tweede man, Van Woelderens, de leiding van GS III korte tijd over tot hij eind 1919 burgemeester van Vlissingen werd. Met de leiding van de Nederlandse inlichtingen- en veiligheidsdiensten werd toen belast de reserve-kapitein der infanterie J.W. van Oorschot. Deze had tijdens de Eerste Wereldoorlog bij GS III gediend als liaisonofficier met de buitenlandse, vooral de Britse, militaire attachés.

Van Oorschot rondde de reorganisatie van GS III af met de benoeming van twee ondercommandanten, die leiding moesten geven aan respectievelijk GS IIIA en GS IIIB. Hoofd van de inlichtingendienst GS IIIA, tevens plaatsvervangend hoofd van de sectie, werd de kapitein der infanterie baron Van Voorst tot Voorst. Het hoofd van GS IIIB kreeg, evenals de chef van de Generale Staf zich had toegedacht, een 'tweede pet': hij werd tegelijkertijd hoofd van de CI. Na een korte periode waarin ritmeester C.S. Sixma baron van Heemstra die functie had vervuld, was het kapitein der artillerie T.S. Rooseboom die deze dubbelfunctie van hoofd GS IIIB, tevens hoofd CI, tot aan de Duitse inval in mei 1940 bekleedde.

Het moge duidelijk zijn, dat het inlichtingen- en veiligheidswerk in de periode van ruim twintig jaar tussen de wereldoorlogen, een vooral militaire aangelegenheid was. Dat gold zonder enige twijfel voor de inlichtingen-

kant. Voor en tijdens de Eerste Wereldoorlog was handhaving van de neutraliteit de hoeksteen van de buitenlandse politiek geweest en daarmee richtsnoer voor de militaire inlichtingendienst om met name over de omringende mogendheden in gelijke mate geïnformeerd te zijn. Dat bleef ook in het interbellum de officiële lijn van het buitenlands beleid en daarmee van de Generale Staf. In de praktijk van het inlichtingenwerk echter, was GS III, onder leiding van Van Oorschoot, tegen het einde van de jaren dertig bereid een oogje dicht te knijpen als het ging om Britse spionage tegen het Duitsland van Hitler. Hoever Van Oorschoot bereid was daarin te gaan werd aan het licht gebracht door het 'Venlo-incident'.

Het onder de naam 'Venlo-incident' bekend geworden *Spiel* van de Duitse *Sicherheitsdienst* met de Britse inlichtingendienst MI 6, was in de loop van 1939 begonnen. De vertegenwoordiger in Nederland van MI 6 was in (een wat leek veelbelovend) contact gekomen met vertegenwoordigers van een anti-Hitlergroepering in het Duitse leger. Om die vertegenwoordigers veilig te kunnen ontmoeten leek het neutrale Nederland het aangewezen 'derde land'. Een formeel Brits verzoek om aan een dergelijke ontmoeting op Nederlands grondgebied mee te werken, kon Van Oorschoot niet honoreren. Wel stelde hij een officier van GS IIIA ter beschikking als verbindingsman die zonodig paden kon effenen en obstakels uit de weg ruimen. In ruil daarvoor zou GS III delen in de informatie die het contact met de vermeende oppositionele Duitse militairen zou opleveren.

De afloop van wat men vandaag een *joint operation* zou noemen, is genoegzaam bekend. De 'oppositie' bleek het geesteskind van Walter Schellenberg, hoofd van *Abteilung VI Ausland* van de Duitse *Sicherheitsdienst*. De geplande ontmoeting met vertegenwoordigers van die 'oppositie' aan de grens bij Venlo bleek een valstrik. De Britse medewerkers van MI 6 werden over de

grens gesleurd en de Nederlandse verbindingsman van GS IIIA, de eerste luitenant der infanterie D. Klop, werd in het begeleidend vuurgevecht gedood. Van Oorschoot moest ontslag nemen als hoofd van GS III, omdat het incident op zo pijnlijke wijze aan het licht had gebracht hoe onder zijn verantwoordelijkheid de samenwerking met MI 6 de geloofwaardigheid van de neutraliteitspolitiek was aangetast. Van Oorschoot werd opgevolgd door de man die aan de wieg van GS III had gestaan en de dienst tijdens de Eerste Wereldoorlog had geleid, de inmiddels als luitenant-generaal gepensioneerde Fabius.

Ook het politieke veiligheidswerk was op nationaal niveau in handen van militairen. GS IIIB en CI vormden, zoals eerder gezegd, vooral door de zuinigheid van Binnenlandse Zaken in de praktijk één veiligheidsdienst die – afhankelijk van het onderwerp – in de rapportage aan de minister van Oorlog de aanduiding GS IIIB, en in de berichtgeving aan de minister van Binnenlandse Zaken, de naam CI hanteerde. Overigens was ook hier de praktijk vaak sterker dan de theorie en werden beide benamingen in de rapportage nogal eens door elkaar gebruikt.

Eén ding was wel duidelijk: de veiligheidsdienst hield zich – of het nu was onder de noemer GS IIIB of CI – in het interbellum voornamelijk bezig met het volgen en registreren van de al genoemde 'revolutionaire stroomingen'. Gedurende lange jaren ging het daarbij uitsluitend om organisaties en personen aan de linkerkant van het politieke spectrum – communisten, anarchisten en ook sociaal-democraten. Pas na het aan de macht komen van Hitler ging de dienst ook aandacht besteden aan rechts-extremistische organisaties en personen in Nederland, waaronder in de eerste plaats de Nationaal Socialistische Beweging (NSB) en zijn leden. Bij dit alles moet bedacht worden dat de veiligheidsdienst in Den Haag in de eerste plaats fungeerde als coördinatie- en distributiecentrum van de door de

plaatselijke politiediensten ingewonnen inlichtingen. Het veldwerk, het 'runnen' van agenten en informanten, werd gedaan door de politie, vooral door de inlichtingendiensten van de grote gemeentelijke politiekorpsen.

De praktijk van het 'op kaart brengen' van leden van en rechts- en links-extremistische organisaties – waartoe lange tijd ook de SDAP werd gerekend – bewees zijn nut toen in 1933, na de muiterij op de kruiser *De Zeven Provinciën*, het zogenaamde ambtenarenverbod werd ingesteld. In het Algemeen Rijksambtenaren Reglement (ARAR) werd een artikel 97b opgenomen dat bepaalde dat ambtenaren ontslagen konden worden bij gebleken lidmaatschap van *eene vereniging die om de doeleinden die zij nastreeft, of de middelen die zij aanwendt, de behoorlijke vervulling van zijn plicht als ambtenaar kan in gevaar brengen of schaden*.

In de praktijk betekende deze wat omslachtige formulering dat er twee lijsten kwamen van voor ambtenaren verboden politieke organisaties. Een lijst gold voor de totale Rijksoverheid, de ander voor het departement van Defensie. Op de algemene lijst stonden links- en rechtsextremistische partijen en partijtjes broederlijk bijeen: de CPH, anarchistische en trotskistische groepen, de Nationaal-Socialistische Nederlandse Arbeiderspartij (NSNAP) en ten slotte ook de NSB. Op de defensielijst figureerden bovendien de SDAP en de bij het socialistische Nederlands Vakverbond (NVV) aangesloten vakbonden. Pas in 1938, toen de lijsten herzien moesten worden, werden de sociaal-democratische organisaties van de defensielijst afgevoerd. Dat had ongetwijfeld te maken met het feit dat de SDAP een jaar eerder was afgestapt van zijn politiek van het 'gebroken gewertje' en nu pleitte voor handhaving van de 'Nederlandse weermacht'. Niet iedereen juichte het toe, dat ook de NSB door het ambtenarenverbod werd getroffen. Onder degenen die daar moeite mee hadden waren ook officieren die – voor kortere of lange-

re tijd – met bewondering en waardschijnlijk ook met afgunst zagen hoe in Duitsland, na het aan de macht komen van Hitler, kosten noch moeiten werden gespaard om de *Wehrmacht* uit te breiden en te moderniseren. Van deze groep officieren was de representant bij uitstek de chef van de Generale Staf, H.A. Seijffardt. Hij was lid van de NSB geweest, maar had zijn lidmaatschap opgezegd omdat hij dan 'meer kon doen'. Een van de dingen die hij daarbij op het oog had, was het ontcrachten van het ambtenarenverbod door het registreren van NSB-leden stop te zetten; het middel daartoe was het naar zijn hand zetten van de veiligheidsdienst.

Het was Seijffardt bij zijn aantreden als chef van de Generale Staf opgevallen dat er bij de Centrale Inlichtingendienst uitsluitend militairen werkten, maar dat hij over deze dienst formeel geen enkele zeggenschap had: de CI viel immers onder de minister van Binnenlandse Zaken. Seijffardt stelde daarom de minister van Defensie voor, ook de CI onder zijn bevelen te plaatsen. Daarbij merkte hij niet ten onrechte op dat de CI in naam een civiele, maar in de praktijk een militaire dienst was, bemand door militairen en geleid door officieren. Van Oorschoot, hoofd van GS III en daarmee ook van de veiligheidsdienst, verzette zich met hand en tand tegen Seijffardts opzetje. Toen deze laatste in 1934 met pensioen ging, ressorteerde de CI nog steeds onder Binnenlandse Zaken en werden leden van de NSB nog steeds geregistreerd. Dit bleef zo tot de Duitse inval.

Het registreren van extremistische personen was niet alleen een instrument om het ambtenarenverbod te kunnen effectueren, het diende ook een ander doel, namelijk het zonodig interneren van staatsgevaarlijke personen. In 1938 had de Ministerraad besloten dat met de voorbereiding daarvan een begin moest worden gemaakt. Die voorbereidingen bestonden er uit, dat de veiligheidsdienst en de plaatselijke politiediensten in onderling overleg lijsten aanlegden

van te arresteren en te interneren personen. Toen op 19 april 1940 de staat van beleg werd afgekondigd, werd de chef van de Generale Staf H.G. Winkelman, opperbevelhebber van land- en zeemacht (OLZ) en belast met het uitvoeren van het Militair Gezag. Ten aanzien van de interneringen bepaalde hij, dat daarvoor alleen personen in aanmerking kwamen van wie de staatsgevaarlijkheid vaststond. Een algemene gezindheid, blijkend uit bijvoorbeeld het lidmaatschap van de CPH of de NSB, vond hij niet voldoende.

onderwerp van dit artikel betreft, aan de hegemonie van de Generale Staf op het gebied van inlichtingen en veiligheid. Tijdens de eerste jaren van de oorlog kwamen de militairen er zelfs in het geheel niet aan te pas; pas na enkele jaren ontstond er op dit gebied een soort van evenwicht.

Na de ineenstorting van de Nederlandse defensie besloot de regering op 13 mei haar zetel naar Londen te verplaatsen. Daar kwamen het staats-hoofd en het kabinet-De Geer op 14 mei aan. Al ras kwam men tot de ont-



Lange Voorhout in Den Haag: ooit een locatie van de BVD

De veiligheidsdienst maakte daarop een nieuwe lijst van eenentwintig personen, achttien nationaal-socialisten en drie communisten. Zij werden op 4 mei 1940 op bevel van Winkelman daadwerkelijk gearresteerd en geïnterneerd.

### De Tweede Wereldoorlog

De Duitse inval op 10 mei 1940 maakte aan veel zaken een eind: aan de Nederlandse onafhankelijkheid, aan de neutraliteitspolitiek en, wat het

dekking dat men elke vorm van informatie over het nu bezette Nederland miste. Van GS III als organisatie was niets over; de archieven van de dienst waren vernietigd; van een *stay behind*-organisatie – voor zover daarvan al serieus sprake was geweest – was niets terechtgekomen door de nasleep van het Venlo-incident. De netwerken van de Britse inlichtingendienst MI 6 waren door datzelfde Venlo-incident, maar vooral door Duitse penetratie van de organisatie in Nederland, van geen enkele bete-

kenis meer. Noch de Nederlanders, noch de Engelsen konden half mei 1940 iets zinnigs naar voren brengen over de toestand in bezet Nederland. Het was dus zaak zo snel mogelijk weer een goed werkende inlichtingendienst van de grond te krijgen.

Hoe slecht het uitwijken naar Londen was voorbereid blijkt ook uit de gang van zaken rond de oprichting van zo'n dienst. Toen de regering in Londen aankwam was daar al aanwezig het voormalige hoofd van GS III Van Oorschot, nu als hoofd van een militaire missie die contact moest leggen met het *War Office*. Tegelijk met de regering waren drie officieren van de inlichtingendienst GS IIIA in Londen aangekomen: het hoofd, majoor der infanterie J.G.M. van de Plassche met twee medewerkers, de kapiteins C.M. Olifiers en L.J.A. Schoonenberg. Zij hadden toestemming tot evacuatie gekregen, omdat hun namen op een Duitse *Fahndungsliste* bleken te staan. Gedrieën meldden zij zich als vanzelfsprekend bij hun oude chef Van Oorschot, nu generaal Fabius met de rest van GS III in bezet gebied was achtergebleven. Onder Van Oorschots leiding togen zij aan het werk. Het meest urgent op dat moment was het onderzoek naar de betrouwbaarheid van de eerste Engelandvaarders en van landgenoten die door de Engelsen ('*better safe than sorry*') waren geïnterneerd bij gebrek aan voldoende gegevens. Daardoor ontstonden al snel contacten met de Britse veiligheidsdienst MI 5. Op verzoek van deze dienst stelde de 'dienst-Van Oorschot' onder meer een rapport op over de rol van de zogenaamde 'vijfde colonne' in Nederland. Werk genoeg dus, zelfs zoveel dat Van Oorschot minister van Defensie A.Q.H. Dijkhoorn benaderde met het verzoek om meer personeel. Tot zijn verbazing verwees de minister hem naar Van 't Sant, die na zijn carrière bij de politie, particulier secretaris van koningin Wilhelmina was geworden en die nu tevens hoofd bleek te zijn van de, buiten Van Oorschot om, inmiddels opgerichte Centrale Inlichtingendienst (CID).

De CID, die zowel de inlichtingen- als de veiligheidstaak kreeg opgedragen, was opgericht bij geheim Koninklijk Besluit van 19 juli 1940 en viel op aandringen van koningin Wilhelmina onder de politieke verantwoordelijkheid van de minister van Justitie P.S. Gerbrandy. Dat Van 't Sant deze dienst ging leiden, kan eveneens aan haar invloed worden toegeschreven. De vakmensen van GS III stonden door dit alles buiten spel.

Het ging de CID niet voor de wind. Van 't Sant werd door velen, onder wie ook bewindslieden, niet vertrouwd en moest het veld ruimen. Als waarnemend hoofd ging R.P.J. Derksema optreden; toen dat geen succes bleek werd luitenant-kolonel der mariniers M.R. de Bruijne, die al hoofd was van het Bureau Voorbereiding Terugkeer, tegelijkertijd tijdelijk hoofd van de CID. Merkwaardigerwijs was in deze periode minister van Binnenlandse Zaken H. van Boeyen, voor de dienst politiek verantwoordelijk. Pas tegen het eind van het jaar 1942 kwam er, na allerhande plannenmakerij, bureaucratische oor-

logvoering en competentiekwesties, een zekere stabiliteit in de organisatie van de inlichtingen- en veiligheidsdiensten. De oorspronkelijke CID werd gesplitst in twee aparte diensten. Het veiligheidsdeel, nog steeds onder leiding van Derksema, keerde als Afdeling Politie (meestal Politie Buitendienst genoemd) terug onder de vleugels van de minister van Justitie. Voor de inlichtingentaak werd een nieuwe dienst in het leven geroepen. Bij KB van 28 november 1942 werd het Bureau Inlichtingen der Nederlandsche Regeering (BI) opgericht onder politieke verantwoordelijkheid van de minister van Oorlog.

Hoofd van BI werd reserve-majoor der artillerie H.G. Broekman, die wegens ziekte al snel zijn functie moest neerleggen. Hij werd opgevolgd door de voormalige kapitein bij GS III, nu majoor der infanterie KNIL dr. J.M. Somer. Deze zou tot het eind van de oorlog BI blijven leiden bij de uitvoering van zijn taak, politieke, economische en militaire inlichtingen over bezet Nederland in te winnen. Hoewel BI ressorteerde onder de



Villa Windekind, privédomein van François van 't Sant

minister van Oorlog, werkte de dienst voor de gehele regering.

Met Somer was eindelijk weer een man 'uit het vak' belast met de leiding van het inlichtingenwerk. Uiteraard in nauwe samenwerking met de Britse MI 6, werden onder zijn leiding agenten naar bezet Nederland gezonden. Die legden enerzijds contacten met al bestaande illegale inlichtingengroepen in bezet gebied zoals die van de Ordedienst (OD); anderzijds richtten zij nieuwe inlichtingengroepen op zoals de groep-Albrecht. De resultaten daarvan kwamen de geallieerde oorlogvoering, maar ook de informatiepositie van de Nederlandse regering in ballingschap, ten goede. Al met al was BI, zeker in vergelijking met de CID, redelijk succesvol.

### De eerste naoorlogse jaren

Op de vraag hoe het na de Duitse nederlaag nu verder moest met de inlichtingen- en veiligheidsdiensten, kwam niet direct een eensluidend antwoord. Ook op dit terrein strenden herstel en vernieuwing om voorrang. Aan de ene kant waren er de Londense ervaringen die in grote mate richtinggevend zouden blijken voor de twee nieuw op te richten 'civiele' diensten: de uit het Bureau voor Nationale Veiligheid voortgekomen Centrale Veiligheidsdienst (CVD) en de Buitenlandse Inlichtingendienst (BID). Aan de andere kant dachten nog steeds velen, en niet alleen in militaire kring, aan herstel van de vooroorlogse situatie waarin GS III een centrale rol had gespeeld. Competentiekwesties tussen met name de departementen van Oorlog, Justitie en Binnenlandse Zaken, bepaalden enkele jaren lang het beeld. Pas het Koninklijk Besluit van 8 augustus 1949 bracht een zekere rust in de situatie.

In de periode kort voor en direct na de bevrijding, had de zorg voor rust en veiligheid de absolute voorrang. Dat gold voor de geallieerde troepen op Nederlands grondgebied die beveiliging eisten tegen eventuele Duitse

Het eerste gebouw van de CVD aan de Javastraat



stay behind-activiteiten; dat gold ook voor het Militair Gezag, dat ervoor diende te waken dat de overgang naar een regulier Nederlands bestuur zonder incidenten zou verlopen. De herinnering aan november 1918 was nog altijd niet verdwenen. Om aan deze veiligheidsbehoeften te voldoen werd de Londense Politie Buitendienst, onder leiding van Derksema, omgevormd tot de sectie III van het Militair Gezag, maar al spoedig bleek dat Derksema niet de man was om een dergelijk apparaat te leiden. De samenwerking met de geallieerden liet te wensen over, maar ook die met de verschillende verzetsgroepen die ieder voor zich contact zochten met de Engelse en Amerikaanse *field security*-eenheden. Er moest, zo vonden de zo langzamerhand weer in Den Haag binnengedruppelde bewindslieden, een organisatie komen die enige coördinatie zou brengen in de relaties tussen het verzet en de geallieerden,

zo mogelijk onder leiding van iemand die voldoende gezag had om die samenwerking ook af te dwingen. Men kwam ten slotte uit op de voormalige korpschef van de Rotterdamse politie L. Einthoven, die werd belast met de leiding van een door hem op te richten Bureau voor Nationale Veiligheid (BNV). Bij beschikking van de chef staf van het Militair Gezag, H.J. Kruls, kreeg het BNV de zorg voor de 'in- en uitwendige veiligheid' opgedragen.

Einthovens eerste zorg was nu ook daadwerkelijk al die verzetsgroepen onder de BNV-paraplu samen te brengen die tot dan toe op eigen houtje met de geallieerden hadden samengewerkt. Daarbij was het hem niet zozeer te doen om hun prestaties en kwaliteiten, hoe voortreffelijk soms ook, maar in de eerste plaats om de door deze groepen tijdens de laatste oorlogsjaren aangelegde documenta-



ties over de inlichtingen- en veiligheidsdiensten van de bezetter zoals de *Abwehr*, de *Gestapo* en de *Sicherheitsdienst*. Deze gegevens waren essentieel voor de uitvoering van de meest urgente taak van het BNV: het identificeren, opsporen, verhoren en eventueel aan de Bijzondere Rechtspleging overdragen van al diegenen die met die Duitse diensten te maken hadden gehad. Tegelijkertijd pakte het BNV de draad weer op van de vooroorlogse veiligheidsdienst: het in de gaten houden van politieke extremisten, zowel aan de linker- als aan de rechterkant.

Terwijl het BNV, dat als tijdelijke organisatie was bedoeld, zijn werk deed werd er rond de jaarwisseling 1945-1946 al nagedacht over een meer permanente oplossing. Het kabinet-Schermerhorn besloot een nieuwe veiligheidsdienst in het leven te roepen, naast een nieuwe buitenlandse inlichtingendienst. Als voorbeeld dienden hierbij de Britse veiligheidsdienst MI 5 en de inlichtingendienst MI 6. Eindhoven kreeg de opdracht uit het personeel van het BNV de meest bekwame en integere krachten te selecteren, om daaruit een nieuwe veiligheidsdienst te vormen die Centrale

Veiligheidsdienst (CVD) zou gaan heten. Somers rechterhand en plaatsvervanger bij BI, C.L.W. Fock, werd belast met het oprichten en leiden van een nieuwe inlichtingendienst naar Brits model. Bij geheime Koninklijke Besluiten van respectievelijk 9 april en 19 februari 1946, werden de Centrale Veiligheidsdienst en de Buitenlandse Inlichtingendienst (BID) in het leven geroepen, beide politiek aangestuurd door de minister-president.

In de militaire sfeer intussen werd gedacht in termen van herstel van de vooroorlogse situatie, zij het met inachtneming van de tijdens de oorlog geleerde lessen. Bij de Generale Staf werden weer secties IIIA en IIIB ingesteld. Bovendien had Somer die bijna twee en een half jaar lang BI had geleid, over de *lessons learned* uitgesproken ideeën. Hij pleitte voor een geheime operationele militaire inlichtingendienst IIIC, die de benodigde informatie zou aandragen voor met name IIIA, en die bovendien bij een eventueel nieuw militair conflict als *stay behind*-organisatie zou kunnen optreden. Daarmee zou het gehannes voorkomen worden dat de eerste jaren in Londen had gekenmerkt.

Somers plannen stuitte voor een belangrijk deel op het verzet van zijn voormalige ondergeschikte Fock. Deze had zich als hoofd van de BID het exclusieve recht verworven van het opereren in het buitenland. Toen hij dan ook lucht kreeg van Somers plannen om ook agenten en informanten naar het buitenland te sturen, stak hij daar, met het gezag van de minister-president achter zich, een stokje voor. Somer werd teruggefloten; hij ging zich toeleggen op de *stay behind*-taak, maar werd al spoedig overgeplaatst naar Nederlands-Indië waar hij hoofd werd van de Centrale Militaire Inlichtingendienst (CMI).

Zo leek enkele jaren na de oorlog een nieuwe stabiele toestand bereikt. Er functioneerden twee civiele diensten ressorterend onder de minister-president; de chef van de Generale Staf beschikte evenals voor de oorlog over een inlichtingen- en een veiligheidssectie GS IIIA en GS IIIB. Nieuw in de militaire sfeer was Somers GS IIIC; bovendien deed de marine bescheiden pogingen om te komen tot een eigen inlichtingendienst. Stabiel was de situatie echter allerminst. Dat had niet zozeer te maken met de militaire diensten, als wel met het feit dat in de civiele sfeer de competentiestrijd nog niet was uitgewoed.

Die competentiestrijd speelde zich vooral af tussen de CVD en het departement van Justitie. Al voor de oorlog had Justitie – en dan vooral de procureurs-generaal – zich na het Venloincident een meer prominente plaats veroverd bij de bestrijding van spionage. De nieuw opgerichte CVD stond er aan in de weg, deze draad weer op te pakken, hetgeen de hartelijke samenwerking tussen Einthovens dienst en Justitie, waaronder ook de Rijkspolitie viel, niet bepaald bevorderde. Toen bovendien in de loop van 1946 een campagne tegen Eindhoven en het BNV op gang kwam, ging Eindhoven tot de aanval over. Hij vroeg minister-president Beel, die inmiddels Schermerhorn was opgevolgd, een commissie in te stellen die zou onderzoeken hoe het BNV onder



Hotel Des Indes: 23 mei 1945, beslissing tot oprichting BNV

Eindhoven had gefunctioneerd, en die bovendien aanbevelingen zou doen over de vraag onder welk departement de CVD zou moeten ressorteren. De gevraagde commissie kwam er in de vorm van de commissie-Wijnveldt, genoemd naar de voorzitter ervan, de advocaat-generaal bij de Hoge Raad J. Wijnveldt. Het oordeel van deze commissie was voor Eindhoven teleurstellend. De commissie prees weliswaar Eindhoven's werkkraft, maar was van oordeel dat het BNV door Eindhoven's gebrekkige leiding in de vernieling was geraakt. In een CVD onder Eindhoven zag de commissie dan ook niets. Zij pleitte voor de instelling van een nieuwe veiligheidsdienst onder de chef van de Generale Staf; de naam van die dienst zou GS IIB moeten zijn. Duidelijker aanhaken bij de vooroorlogse situatie was nauwelijks denkbaar.

Dat Eindhoven met dit rapport niet blij was is één ding; dat Beel zich er niet bij neerlegde was belangrijker. In tegenstelling tot de commissie-Wijnveldt had Beel namelijk wel waardering en zelfs bewondering voor Eindhoven gekregen. Bovendien wilde hij als minister-president, tevens minister van Binnenlandse Zaken, de CVD niet kwijt. Hiertoe wierp hij een beproefd middel in de strijd: een nieuwe commissie, ditmaal de commissie-Prinsen. Die zou het werk van de commissie-Wijnveldt moeten afronden (eigenlijk overdoen) en richtlijnen moeten ontwerpen voor de samenwerking tussen de CVD en politie en Justitie.

De voorzitter M.J. Prinsen was secretaris-generaal van Binnenlandse Zaken; verder zat Fock in de commissie, inmiddels in zijn nieuwe kwaliteit van raadadviseur in algemene dienst bij Algemene Zaken; voorts de secretaris-generaal van Justitie J.C. Tenkink, de chef van Marinestaf, E.J. van Holthe en de chef van de Generale Staf Kruls. Beslissend voor de adviezen van de commissie waren niet zozeer rationale argumenten, als wel het feit dat minister-president W. Drees, sinds juli 1948 Beels opvolger, totaal

niet met Eindhoven overweg kon. Dat had te maken met beider botsende persoonlijkheden, maar toch ook met het feit dat Eindhoven deel had uitgemaakt van het zogenaamde Driemanschap van de Nederlandse Unie. Drees' afkeer van Eindhoven ging zo ver dat raadadviseur, later secretaris-generaal, Fock hem moest overreden Eindhoven überhaupt nog te ontvangen. Fock's suggestie, de CVD 'over te doen' aan Binnenlandse Zaken waar Prinsen de dienst maar al te graag onder zijn vleugels zou nemen, vond bij Drees dan ook een willig oor. Fock kreeg (en nam) in de commissie-Prinsen de ruimte om een oplossing in die richting te stimuleren. De beide militairen onthielden zich wat de CVD betreft van commentaar, zodat Fock en Prinsen samen Tenkink konden overstemmen. In het rapport van de commissie is deze gang van zaken terug te vinden.

De kern van de in het rapport-Prinsen verwoorde aanbevelingen werd gevormd door de redenering, dat elk departement zijn eigen inlichtingen en/of veiligheidsdienst zou moeten hebben. Niet geheel consequent betekende dat volgens het rapport, dat de Buitenlandse Inlichtingendienst onder Algemene Zaken zou blijven ressorteren, dat de CVD onder Binnenlandse Zaken zou komen en dat de departementen van Marine en Oorlog de beschikking zouden krijgen over respectievelijk de Marine Inlichtingendienst (MARID) en de Militaire Inlichtingendienst (MID). De luchtmacht was op dat moment nog geen zelfstandig krijgsmachtdeel. De activiteiten van al die diensten zouden op elkaar afgestemd moeten worden door een Coördinatie Commissie, zo mogelijk onder voorzitterschap van de minister-president. De aanbevelingen van de commissie-



**Mr. L.  
Eindhoven:  
grondlegger  
van de naoorlogse veiligheidsdienst**

Prinsen, inclusief de daaraan ten grondslag liggende redeneringen, werden door het kabinet overgenomen. Zij vormden de basis voor het Koninklijk Besluit van 8 augustus 1949, dat voor praktisch de gehele duur van de Koude Oorlog de vormgeving vastlegde van de Nederlandse *intelligence community*.

## Koude Oorlog

Het jaar 1949 was voor de Nederlandse buitenlandse politiek en derhalve ook voor de defensiepolitiek, van groot belang. Nog maar net bekomen van de Tweede Wereldoorlog had ons land te maken gekregen met een naar onafhankelijkheid strevend Nederlands-Indië. Nog voordat – na de koloniale oorlogen die toentertijd eufemistisch 'politieacties' heetten – de soevereiniteit over de archipel aan de Republiek Indonesia was overgedragen, was in datzelfde jaar 1949, de Koude Oorlog als het ware geïnstitutionaliseerd door de oprichting van de NAVO. Nederland was van het Noord-Atlantisch verbond vanaf het begin een overtuigd en trouw lid, overtuigd als het was van de noodzaak zich tegen de expansieve Sovjet-Unie teweer te stellen. Voor de komende decennia zou de Koude Oorlog maat- en richtinggevend zijn voor het buitenlands beleid van Nederland, zowel op diplomatiek als op militair gebied. De oriëntatie en activiteiten van de inlichtingen- en veiligheidsdiensten, zowel de civiele als de militaire, vormden daarvan een afspiegeling.

1949 was het jaar waarin de *intelligence community*, op basis van het rapport van de commissie-Prinsen, zijn vorm en samenhang kreeg. Oorspronkelijk gecoördineerd door een commissie onder leiding van de minister-president, vanaf 1956 door een gepensioneerd vlagofficier die de titel coördinator van de Inlichtingen- en Veiligheidsdiensten kreeg, bestond de Nederlandse inlichtingengemeenschap aanvankelijk uit vier diensten: twee civiele en twee militaire. Onder



'Ik heb de mol gevonden...'

de minister-president functioneerde de Buitenlandse Inlichtingendienst (BID); onder de minister van Binnenlandse Zaken de nu Binnenlandse Veiligheidsdienst (BVD) geheten dienst onder leiding van Einthoven. De minister van Marine was politiek verantwoordelijk voor de MARID, zijn collega van Oorlog voor de MID. Voor alle diensten gold dat gedurende vier decennia de eisen en omstandigheden van de Koude Oorlog hun *targets* en *modus operandi* bepaalden. Wellicht is dit de plaats om zeer in het kort in te gaan op het functioneren van de desbetreffende diensten in die periode.

De BVD groeide onder de dynamische leiding van Einthoven op een explosieve manier. De dienst moest enerzijds het binnenlands communisme in kaart brengen als potentiële vijfde colonne van het Rode Leger, en anderzijds spionage vanuit de landen van het Warschau Pact onderkennen en tegengaan. Bij de personele en materiële beveiliging van overheid en bedrijfsleven, inclusief de bedrijven die voor defensie werkzaam waren, speelde de BVD een centrale rol. Een grote afdeling opleidingen waar niet

alleen eigen personeel, maar ook dat van de politie en van marine en luchtmacht (niet van de landmacht!) cursussen volgde, droeg bij aan die centrale rol. In de jaren zeventig bereikte de dienst een omvang van ruim zevenhonderd personeelsleden.

Voor de BID lag het allemaal wat anders en moeilijker. Onder het direct toezicht van de minister-president was er ten aanzien van deze dienst altijd grote zuinigheid betracht, zeker onder het bewind van Drees. Achtereenvolgende ministers van Algemene Zaken huldigden de opvatting, dat hun departement het voorbeeld moest geven als het aankwam op zuinig omgaan met middelen en mensen. Het gevolg daarvan was, dat de dienst die eigenlijk nooit boven zijn geboortegewicht van enkele tientallen medewerkers is uitgekomen, ook nooit echt een kans heeft gekregen uit te groeien tot een volwaardige inlichtingendienst. De resultaten konden dan ook nauwelijks anders dan teleurstellend zijn. In de jaren zeventig is nog even geprobeerd de dienst als uitsluitend operationeel orgaan en als zelfstandig onderdeel onder te brengen bij de minister van Defensie. Dat bleek al

helemaal niet te werken, waarna de dienst als Inlichtingendienst Buitenland terugkeerde onder de vleugels van Algemene Zaken en daar aanvankelijk met enig succes functioneerde. Toen in de jaren tachtig door zwakke sturing vanuit Algemene Zaken en door opgelegde relatief grote personele bezuinigingen, onderlinge tegenstellingen tussen (ex-)militairen en 'burgers' een vernietigende omvang konden bereiken, gleed de dienst af naar een nieuw dieptepunt. Het einde van de Koude Oorlog maakte de roep om het 'vredesdividend' te verzilveren onweerstaanbaar en veroorzaakte verdere krimp in de omvang van het personeel en nieuwe interne proble-

Muur, eist enige toelichting. Het KB van 8 augustus 1949 bepaalde dat de minister van Marine politiek verantwoordelijk was voor de MARID en de minister van Oorlog voor de MID. Op het moment van inwerkingtreden van het KB werden beide ministersposten bekleed door één en dezelfde minister, W.F. Schokking. Toen bovendien in 1951 de Koninklijke Luchtmacht een zelfstandig krijgsmachtdeel werd kreeg ook zij een eigen inlichtingendienst, de Luchtmacht Inlichtingendienst (LUID). Ook het hoofd van deze dienst viel onder de minister van Oorlog. In de praktijk betekende een en ander dat één minister, in dit geval C. Staf, die bijna negen jaar minister

de staven van de respectieve krijgsmachtdelen. Zij vielen namelijk in de praktijk grotendeels samen met de secties inlichtingen en veiligheid van die staven, hoewel er tussen de diensten en de stafsecties theoretisch onderscheid werd gemaakt. Volgens die theorie waren de diensten de zogenaamde verzamelorganen van de gegevens, die door de stafsecties tot inlichtingen- en veiligheidsrapportages werden verwerkt. In de praktijk echter was dat onderscheid niet of nauwelijks te maken: de hoofden van de MID, MARID en LUID waren tegelijkertijd hoofden van de stafsecties, terwijl ook het personeel in overgrote meerderheid tot beide organisaties behoorde. In deze matrixachtige constructie van de 'twee petten' (daar zijn ze weer!) vielen inlichtingendiensten en stafsecties in wezen samen. En dat betekende vervolgens dat de hoofden van die diensten, hoewel formeel direct onder de minister van Defensie vallend, in de praktijk van alledag hun bevelen en aanwijzingen – direct of indirect – ontvingen van hun respectieve bevelhebbers. De diensten waren in essentie 'bevelhebbersdiensten' geworden. De MARID richtte zich op het inwinnen van inlichtingen over met name de vloten van de Sovjet-Unie en andere communistisch geregeerde landen; de MID – vanaf 1972 LAMID – trachtte in de eerste plaats te voorzien in de inlichtingenbehoeften van het Eerste Legerkorps, dat in de Noord-Duitse Laagvlakte de eerste klap van de aanstormende Russische tanks zou moeten opvangen; de LUID richtte zich op het in kaart brengen van vijandelijke vliegvelden achter het IJzeren Gordijn en het op de hoogte blijven van ontwikkelingen in de militaire luchtvaart daar. De veiligheidscomponenten van de diensten screenden hun beroepspersoneel en dienstplichtigen, waarbij de aandacht vooral uitging naar communistisch gezinde personen. LUID en MARID deden dat in nauwe samenwerking met de BVD, die LAMID had daarvoor een omvangrijke eigen organisatie, ook al omdat het leeuwendeel van de dienstplichtigen bij de landmacht terechtkwam.



**BVD-gebouw aan de President Kennedylaan te Den Haag (1956-1993)**

men. Toen die problemen door 'leken' naar buiten kwamen, hief minister-president Lubbers de dienst per 1 januari 1994 op. Voor zover dat wettelijk mogelijk was werden de taken van de dienst verdeeld over de BVD en de MID.

Het bestaan van twee, na korte tijd drie afzonderlijke militaire inlichtingendiensten gedurende bijna de gehele periode tot de val van de Berlijnse

van Oorlog en Marine is geweest, als enige verantwoordelijk was voor de drie militaire inlichtingendiensten.

Toen de ministeries van Oorlog en Marine in 1959 werden samengevoegd tot ministerie van Defensie, kwam niemand op de gedachte dat dit wellicht een goed moment was om de drie diensten te centraliseren. Daarvoor waren de drie diensten inmiddels ook teveel onderdeel geworden van

## De Wet op de Inlichtingen- en Veiligheidsdiensten

De beschreven constructie van het samenstel van inlichtingen- en veiligheidsdiensten zoals dat in 1949 vorm kreeg, heeft het bijna vier decennia uitgehouden. Pas tegen het einde van de Koude Oorlog opende onder zware politieke druk, de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) in 1987, de weg naar nieuwe verhoudingen in de inlichtingenwereld. De wet die per 1 februari 1988 in werking trad bepaalde namelijk dat er, naast de BVD en (toen nog) de IDB, slechts één militaire inlichtingendienst zou zijn. Binnen de diensten was al een beweging gaande in de richting van hechtere samenwerking, maar dat de Kamer vrijwel unaniem samensmelting van de bestaande drie militaire diensten eiste, had te maken met een incident dat in de eerste plaats de veiligheidsafdeling van de LAMID trof. In 1984

had de anti-militarische organisatie 'Onkruit' bij een inbraak in een Utrechtse kazernes, documenten ontvreemd waaruit een verre gaande bemoeienis van de LAMID met 'Onkruit' en andere soortgelijke organisaties, waaronder vredesbewegingen, naar voren kwam. De documenten werden gepubliceerd, hetgeen leidde tot politieke commotie en vragen in de Tweede Kamer aan de minister van Defensie. Dit alles speelde zich af voor en tijdens de behandeling van het voorstel van de Wet op de Inlichtingen- en Veiligheidsdiensten, waardoor de minister van Defensie het zwaar te verduren kreeg bij het verdedigen van het oorspronkelijke voorstel, de drie afzonderlijke diensten te handhaven. Onder druk van de Kamer ging de minister, J. de Ruyter, door de bocht, overigens zeer tegen de zin van de bevelhebbers, en stemde in met samensmelting van de drie diensten tot één gecentraliseerde militaire inlichtingendienst.

Dat wil niet zeggen dat die ene dienst er nu ook dadelijk was. Het eiste een reeks van grote en kleine reorganisaties, touwtrekkerij en compromissen, voordat de MID aan zijn huidige (laatste?) reorganisatieproces kon beginnen. De bedoeling is dat de MID na afronding daarvan een geïntegreerde militaire inlichtingen- en veiligheidsdienst zal zijn, die zowel de politieke en ambtelijke top van het departement adequaat kan bedienen als de bevelhebbers van de krijgsmachtdelen.

Als het zover is zal tenslotte toch bereikt worden wat H.A.C. Fabius al in 1921 bepleitte in de *Militaire Spectator*: een centrale dienst voor het gehele defensieapparaat. 'Alleen een dergelijke dienst', aldus Fabius in zijn geliefde spreekbuis, 'is in staat onderscheid te maken tussen ware en onware berichten'. Stellig was hij daarom in zijn mening dat

*'de beoordeling van alles wat maar in ver verwijderd verband staat met militaire politiek of strategie behoort te zijn in eene hand'.*

### Tot slot

Op het moment dat deze *Militaire Spectator* verschijnt is de parlementaire behandeling van het nieuwe ontwerp van de Wet op de Inlichtingen- en Veiligheidsdiensten nog gaande of vrijwel afgerond. Waar het hier om gaat is dat deze wet als het ware een nieuw evenwicht creëert tussen de civiele en militaire inlichtingen- en veiligheidsdiensten. Bij inwerkingtreden van de wet telt ons land nog twee diensten: de civiele Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). In de nieuwe benamingen voor respectievelijk de huidige BVD en MID, komt tot uiting dat beide diensten zowel een (buitenlandse) inlichtingentaak als een veiligheidstaak hebben. De erfenis van de opgeheven IDB is daarmee definitief verdeeld.

### Literatuur

- F.A.C. Kluiters – *De Nederlandse inlichtingen- en veiligheidsdiensten*. SDU, Den Haag, 1993.
- D. Engelen – *Geschiedenis van de Binnenlandse Veiligheidsdienst*. SDU, Den Haag, 1995.
- D. Engelen – *Inlichtingendienst Buitenland*. PIVOT-rapport nr. 30, Den Haag, 1996.
- B. de Graaff, C. Wiebes – *Villa Maarheeze. De geschiedenis van de inlichtingendienst buitenland*. SDU, Den Haag, 1998.
- D. Engelen – *De Militaire Inlichtingendienst 1914-2000*. SDU, Den Haag, 2000.

## DE MILITAIRE SPECTATOR

1021

Waarin de boodschap van Fabius

# De Militaire Inlichtingendienst, vandaag en morgen

J.A. van Reijn – generaal-majoor der mariniers\*

## Inleiding

Sinds 1 augustus 2000 is de MID in een nieuwe jas gestoken. Per die datum heeft de dienst een forse reorganisatie ingezet. Strategie, structuur en werkprocessen zijn op de schop gegaan. Ook is een proces van concentratie op een kleiner aantal locaties van start gegaan. Alle Haagse elementen van de nieuwe dienst zijn nu ondergebracht in gebouw 32 op de Frederikkazerne. Voor een ander deel van de dienst, met name de afdeling verbindingsinlichtingen, is het proces van samenvoeging en concentratie nog in volle gang. Bij deze reorganisatie van de MID zijn ruim tweehonderdvijftig van de omstreeks zeventig honderd functies ingrijpend gewijzigd. Gedwongen ontslagen hebben niet plaatsgehad.

Tezelfdertijd is een veranderingsprogramma ingezet onder de naam PRISMA om de cultuuromslag te maken van een gesloten, wat verkokerde organisatie, naar een dienst met meer interne samenhang, die integrale en kwalitatief hoogwaardige producten aflevert en die op transparante wijze verantwoording aflegt over zijn handelen aan publiek, opdrachtgevers en behoeftezoekers. De directie Organisatie en Informatievoorziening van het ministerie van Defensie heeft deze



Frederikkazerne te Den Haag, thuisbasis van de MID

reorganisatie inmiddels, een jaar na dato, geëvalueerd. De bevinding op hoofdlijnen is dat de MID weer op koers ligt.

Deze reorganisatie valt samen met een andere belangrijke ontwikkeling: de totstandkoming van een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV). Deze wet gaat de huidige uit 1987 stammende wet vervangen. Het wetsvoorstel ligt thans bij de Eerste Kamer. Volgens deze wet krijgt de MID een nieuwe naam: Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Die naam is voor de dienst van ondergeschikt belang. Inhoudelijk zal de nieuwe wet echter grote invloed hebben op taken, bevoegdheden en verantwoordelijkheden van de beide Nederlandse diensten MID en

BVD. Bij de inregeling van de nieuwe organisatie van de MID wordt hiermee al rekening gehouden.

Met dit artikel beoog ik u in kort bestek over het bovenstaande te informeren.

## Taken

Eerst een blik op de organisatie van Defensie en op de plaats die de MID daarin inneemt (zie organigram 1). De *Defensienota 2000* geeft daarover duidelijkheid:

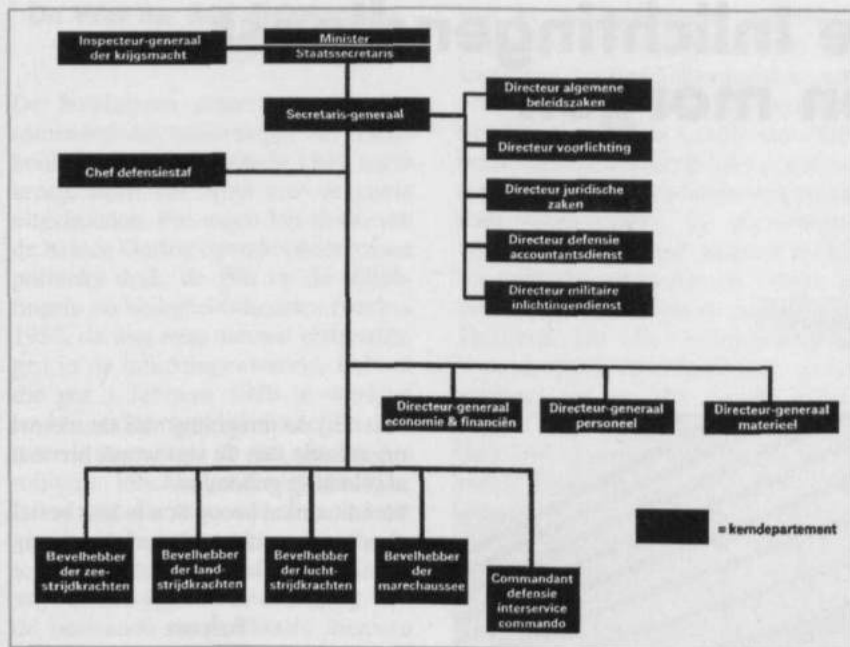
*Hoewel de MID een uitvoerende dienst is, is er vanwege de aard van het werk voor gekozen deze niet op afstand te plaatsen.<sup>1</sup>*

De MID maakt dus deel uit van de Centrale Organisatie en rapporteert door tussenkomst van de secretaris-generaal aan de minister. Doorslaggevend voor deze positionering zijn de bijzondere bevoegdheden van de MID, die om directe politieke aansturing vragen. De minister kan de directeur MID binnen grenzen mandaat verlenen om die bevoegdheden toe te passen. Dat is ook zo bij wet geregeld. In de nieuwe wet komt dat nog sterker tot uitdrukking. Andersom is de directeur gehouden de minister 'bij voortdurend in kennis te stellen van al hetgeen van belang kan zijn'.<sup>2</sup> Dit wil echter niet zeggen dat de MID uitsluitend voor de minister werkt. Onze kring van behoeftezoekers is aanzienlijk breder dan alleen de bewindsman. Kerntaak van de MID is ondersteuning van Defensie – zowel de departementsleiding als de krijgsmacht – met

\* De auteur is directeur van de Militaire Inlichtingendienst.

<sup>1</sup> Tweede Kamer, vergaderjaar 1999-2000, 26 900, nrs 1-2 *Defensienota 2000*, p. 67.

<sup>2</sup> Staatsblad 1987, 635, Wet op de inlichtingen en veiligheidsdiensten, art. 11.



Organigram 1 De defensieorganisatie

adviezen, beoordelingen en rapportages op het gebied van inlichtingen en contra-inlichtingen en veiligheid. De deeltaken van de dienst zijn expliciet opgenomen in de Wet op de Inlichtingen- en Veiligheidsdiensten. De MID voert deze taken op maat en naar behoefte uit. De dienst werkt dus in het kader van indicatie en waarschuwing ook ongevraagd advies geven. De MID produceert in beginsel *vraaggestuurd*, maar kan in het kader van indicatie en waarschuwing ook ongevraagd advies geven. De MID produceert in beginsel *strategische inlichtingen*,<sup>3</sup> dat wil zeggen ter ondersteuning van besluitvorming in het kader van formering, instandhouding en inzet van de krijgsmacht.

Voor zover het in het vermogen van de dienst ligt, produceert de MID ook *operationele inlichtingen*,<sup>4</sup> dat wil zeggen ter ondersteuning van de krijgsmacht bij de planning, voorbereiding en uitvoering van concrete militaire operaties. Maar op dit punt hebben de chef defensiestaf en de bevelhebbers ook eigen verantwoordelijkheden.

<sup>3</sup> *Strategic Intelligence*: US: Intelligence that is required for the formulation of military strategy, policy, and military plans and operations at national and theatre levels (Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0).

<sup>4</sup> *Operational Intelligence*: US: Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theatres or areas of operations (Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0). UK: Intelligence provided directly in support of current and planned operations. It is always focused on a defined operational mission (Joint Operational Intelligence, Joint Warfare Publication 2-00).

Daarnaast verleent de MID ook diensten aan instanties buiten het departement van Defensie, zowel in Nederland als daarbuiten. In Nederland zijn dat bijvoorbeeld de BVD, en de ministeries van Buitenlandse Zaken, Justitie en Algemene Zaken. Buiten Nederland zijn dat bijvoorbeeld internationale organisaties zoals NAVO en EU, alsmede buitenlandse inlichtingen- en veiligheidsdiensten ('partnerdiensten'). De MID is door de aard van zijn taken sterk op het buitenland gericht en ook in het buitenland actief bij de verzameling ('verwerving') van inlichtingen. De dienst hecht dan ook groot belang aan internationale samenwerking en het onderhouden van contacten met de buitenlandse partners.

De deeltaken van de MID zijn op grond van de huidige wet te onderscheiden in een *inlichtingentaak*, en taken op het gebied van *contra-inlichtingen en veiligheid*. Met de nieuwe wet komt daar een deeltaak bij, namelijk een *specifieke inlichtingentaak betreffende het buitenland*. Ten slotte is de MID in Nederland belast met de interceptie van niet-kabelgebonden telecommunicatie, de zogenoemde *verbindinginlichtingen*. Hierna worden deze taken en bevoegdheden kort toegelicht. In buitenlandse inlichtin-



Dagelijkse briefing in het DCBC

genstructuren zijn deze taken overigens vaak ondergebracht in twee of drie afzonderlijke diensten (die soms ook nog onder verschillende departementen ressorteren). Bij de MID worden zij onder één dak uitgevoerd en dat bevordert het maken van integrale, *all source* inlichtingenproducten. De kunst is dan om de dienst ook als één geheel te laten functioneren. Zie hier één van de belangrijke doelstellingen van de reorganisatie.

#### Inlichtingen

Op inlichtingengebied doet de MID onderzoek naar ontwikkelingen in andere landen die mogelijk een risico kunnen opleveren voor de veiligheid van Nederland (al of niet in bondgenootschappelijk verband), en waar de krijgsmacht rekening mee moet houden bij de opbouw van zijn militaire capaciteiten. De MID onderzoekt daartoe zowel intenties als capaciteiten van die landen, dat wil zeggen maakt analyses van politiek/militaire ontwikkelingen, van militair/industriële potentieel, van programma's voor de opbouw van strijdkrachten, van militair/technologische ontwikkelingen en van proliferatie van wapens. Daarnaast onderzoekt de MID ontwikkelingen op het gebied van internationale vrede en veiligheid die mogelijk tot inzet van de Nederlandse krijgsmacht kunnen leiden. Dat wil zeggen wij waarschuwen voor, volgen en beoordelen zich ontwikkelende crises, maken risicoanalyses in verband met mogelijke Nederlandse betrokkenheid en adviseren bij besluitvorming en planning.

Dat onderzoek omvat bronnenonderzoek (deels open-bronnenmateriaal en rapportages van andere diensten), maar ook eigen gesloten bronnen, zoals verbindingsinlichtingen en operationele activiteiten. Concrete producten zijn bijvoorbeeld: de dagelijkse briefing over actuele ontwikkelingen in het Defensie Crisis Beheersings Centrum (DCBC), een dagelijkse inlichtingenrapportage, een wekelijkse inlichtingenrapportage, specifieke rapportages over bepaalde onderwerpen, en het beheer van databases met militair-technische gegevens waarvan



Ook bij het beveiligen van defensie-informatie bij de Nederlandse industrie heeft de MID een taak

de krijgsmacht gebruik kan maken voor planning en operationele doeleinden.

#### Contra-inlichtingen en veiligheid

De MID onderzoekt activiteiten van personen en organisaties die specifiek ten doel hebben de veiligheid of de paraatheid van de krijgsmacht te schaden en die zich daarbij richten op militairen, op militaire objecten of op vertrouwelijke gegevens van de krijgsmacht. Dit laatste omvat ook de veiligheid van de Nederlandse defensie-industrie. Het kan daarbij bijvoorbeeld gaan om buitenlandse inlichtingendiensten, om anti-militaristische actiegroepen, om politiek geïnspireerd rechts extremisme en religieus fundamentalisme. In Nederland wordt in dit taakveld nauw samengewerkt met de BVD. Het onderzoek omvat bronnenonderzoek en contra-inlichtingenoperaties. Concrete producten zijn bijvoorbeeld: tweewekelijkse contra-inlichtingenrapportages en veiligheidsadviezen (juist ook aan commandanten van eenheden). Voorts ondersteunt de MID de eenheden van de Nederlandse krijgsmacht te velde die in het buitenland aan crisisbeheer-

singsoperaties deelnemen met zogenoemde CIV-teams, doorgaans ondergebracht bij het Contingentscommando.

*Debriefing* van uitgezonden personeel is een onderdeel van deze steunverlening. Ten slotte voert de MID veiligheidsonderzoeken uit naar al het defensiepersoneel dat een vertrouwensfunctie vervult of gaat vervullen (bij indiensttreding). Dat zijn zo'n 23.000 veiligheidsonderzoeken per jaar.

#### Inlichtingen buitenland

Een enkel woord over de bijzondere buitenlandtaak, zoals voorzien in de nieuwe wet (WIV). Het gaat om onderzoek naar onderwerpen met een militaire relevantie, zoals opgedragen door de minister-president in overleg met de betrokken ministers (Binnenlandse Zaken en Defensie). Naar verwachting zullen deze onderwerpen in het verleden liggen van de normale inlichtingentaak van de MID, die immers ook op het buitenland is gericht. Daarbij kan gebruik gemaakt worden van de operationele mogelijkheden die de dienst al ten aanzien van het buitenland heeft. Evenals de BVD is de





Interceptie van berichtenverkeer

MID zich thans op deze nieuwe taak aan het voorbereiden.

#### Verbindingsinlichtingen

Ten slotte is de MID belast met verbindingsinlichtingen (VI), het onderscheppen van berichtenverkeer via de ether. De MID doet dit ook ten behoeve van andere belanghebbenden, zoals de BVD. Begin 2000 is een meerjarenprogramma ontwikkeld dat ten doel heeft de interceptiecapaciteit uit te breiden naar nieuwe vormen van telecommunicatie. Ook technologisch blijven door verbetering en vernieuwing van apparatuur, is onderdeel van het programma. Dit vraagt forse investeringen. Tegelijkertijd gaat het hele verbindingsinlichtingenproces doelmatiger en vanaf een kleiner aantal locaties verlopen. En dat levert weer bedrijfseconomische voordelen op. Van de positieve effecten van dit

plan kunnen ook de 'klanten' van VI buiten het departement van Defensie profiteren.

#### Organisatie en werkwijze

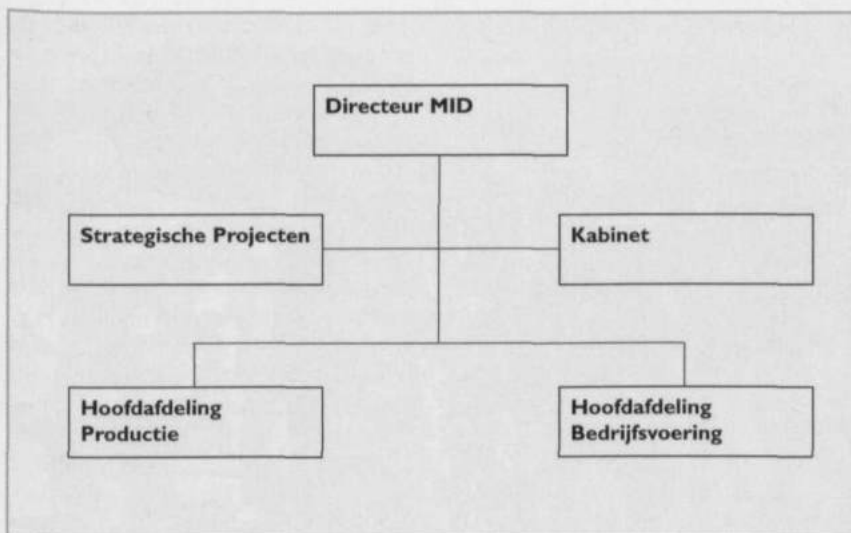
Dan de organisatie. Die omvat circa zevenhonderd functies. Iets meer dan de helft van het personeel is burgermedewerker, de overigen zijn militair. De organisatiestructuur berust op het beginsel van scheiding van productie en bedrijfsvoering (zie organigram 2). Productietaken enerzijds en bedrijfsvoerings- en ondersteunende taken anderzijds, zijn gecentraliseerd in twee afzonderlijke hoofdafdelingen. Aan de productiekant ligt de nadruk op de kerntaak van de MID: het doelmatig en vraaggestuurd leveren van integrale inlichtingenproducten door nauwe samenwerking tussen verwer-

ving en verwerking van inlichtingen en afstemming met de klant. Aan de bedrijfsvoeringskant wordt doelmatigheid bevorderd door bundeling van schaarse expertise en capaciteit. Vanuit de hoofdafdeling bedrijfsvoering worden de productieafdelingen vervolgens op maat en naar behoefte bediend. Dit gebeurt onder andere door zoveel mogelijk projectmatig te werken. Met deze organisatie en werkwijze wordt invulling gegeven aan een tweede belangrijke doelstelling van de reorganisatie, namelijk verbetering van de bestuurbaarheid en beheersbaarheid van de organisatie.

De directeur stuurt de hoofdafdelingen aan en draagt zorg voor de nodige *checks and balances* tussen beide organisatiedelen. De hoofden Productie respectievelijk Bedrijfsvoering zijn beide tevens plaatsvervangend directeur en kunnen elk op hun eigen terrein de dienst met voldoende mandaat vertegenwoordigen. De directeur is voorts verantwoordelijk voor het totale proces van reorganisatie en verandering ('verander manager'). Hiervoor heeft hij de beschikking over de afdeling Strategische Projecten, onder meer belast met projectrapportage, programmabesturing en beleidsvorming op inlichtingengebied. Daar waar dit laatste de internationale (militaire) dimensie betreft, gebeurt dit in nauwe afstemming met de directie Algemene Beleidszaken en de Defensiestaf. De ontwikkeling van een inlichtingenfunctie voor de EU is daarvan een voorbeeld. Voor de verantwoording richting departement en politiek, alsmede voor beleidsmatige interdepartementale afstemming, beschikt de directeur over een klein Kabinet. Jaarverslagen, Kamervragen, periodiek overleg met de minister, voorbereiding van vergaderingen van het directiebestuur, van CVIN<sup>5</sup> en van MICIV<sup>6</sup> enz., zijn onderwerpen die daar berusten.

<sup>5</sup> CVIN: Comité Verenigde Inlichtingendiensten Nederland.

<sup>6</sup> MICIV: Ministeriële Commissie voor Inlichtingen en Veiligheidsdiensten (onderaad van de MR).



Organigram 2 Organisatie MID

### Hoofdafdeling Productie

In de hoofdafdeling Productie (circa 590 functies) zien we allereerst de afdelingen die daadwerkelijk inlichtingen verzamelen (zie organigram 3). De afdeling *Human Intelligence* houdt zich bezig met de exploitatie van menselijke bronnen. De afdeling voert inlichtingenoperaties uit die onder andere ten doel hebben informanten en/of agenten te 'runnen'. De afdeling Verbindingsinlichtingen verwerft inlichtingen door de interceptie van telecommunicatie via de ether. Vanuit enkele locaties in Nederland worden zowel militaire als civiele radio- en satellietverbindingen onderschept. Uit het aldus geïntercepteerde materiaal worden vervolgens door onder andere signaalanalyse, ontcijfering, vertaling en selectie, bruikbare inlichtingen gedestilleerd. De afdeling Contra-inlichtingen en Veiligheid doet contra-inlichtingenonderzoek en operaties, en geeft adviezen op het gebied van militaire veiligheid, industrieveiligheid en informatiebeveiliging.

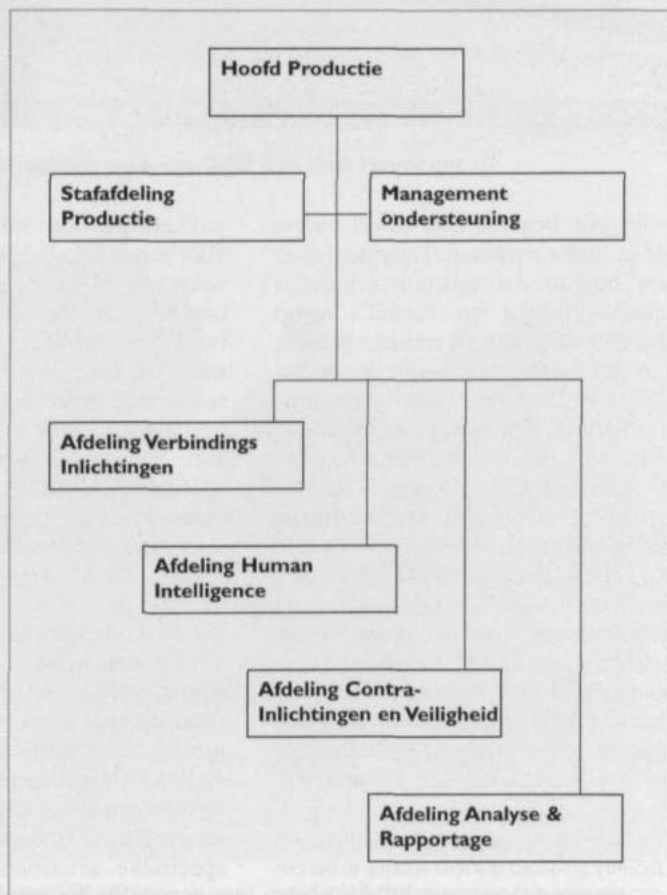
Tevens doet zij veiligheidsonderzoeken naar defensiepersoneel op grond van de Wet op de Veiligheidsonderzoeken (wvo). De afdeling maakt voor een groot deel haar eigen rapportages en producten. Tegelijkertijd

heeft zij ook een verwervende rol ten behoeve van het integrale inlichtingenproces bij de MID. Dat geldt bijvoorbeeld sterk bij de ondersteuning

van uitgezonden eenheden, waar het onderscheid tussen inlichtingen en veiligheid minder telt.

De aldus verzamelde inlichtingen worden verwerkt bij de afdeling Analyse en Rapportage tot voor de 'klant' bruikbare producten. De MID streeft daarbij naar betrouwbaarheid, toegevoegde waarde en toegankelijkheid als belangrijke kwaliteitskenmerken. Voldoende voorspellend vermogen hoort daartoe ook, in het kader van adequate *indication and warning*. Voor de productie van *basic intelligence*<sup>7</sup> kent de afdeling Analyse en Rapportage een aantal regiobureaus waarin deskundigheid en analysecapaciteit zijn gebundeld. De regiobu-

<sup>7</sup> *Basic Intelligence*: Basic Intelligence is the background material on any subject which can be used in the planning of operations and as a basis for evaluating new information or intelligence (STANAG AINTP 1A).



Organigram 3  
Structuur  
hoofdafdeling  
Productie



De MID levert ook een bijdrage aan de voorbereiding van crisisbeheersingsoperaties

reus zijn bemand met zowel burger als militaire analisten. Daarnaast is er een bureau dat militair-technische ontwikkelingen en thema's volgt (zoals proliferatie en militair gebruik van de ruimte) en waar de desbetreffende databases worden beheerd. Een ander belangrijk deel van de afdeling is het OSINT-centrum. OSINT, of *open source intelligence*, is het systematisch verzamelen van informatie uit open bronnen en die verwerken in of tot inlichtingenproducten. Het internet is daarbij een belangrijk medium. Ook IMINT, of *imagery intelligence*, is in de afdeling Analyse en Rapportage terug te vinden. Ten slotte levert de afdeling ook *current intelligence*,<sup>8</sup> dat wil zeggen het volgen en initieel beoordelen van actuele ont-

wikkelingen op inlichtingengebied voor zover van belang voor de eerstvolgende 24 tot 96 uur. De afdeling beschikt daartoe over een *Current Intelligence Unit* (CIU). Die is dag en nacht bemand, 365 dagen per jaar, en is daarmee ook buiten de diensturen het aanspreekpunt voor de gehele MID. Van daaruit wordt bijvoorbeeld ook de dagelijkse inlichtingenbriefing verzorgd in het DCBC, aan de inhoud waarvan overigens de gehele MID bijdraagt.

Uit de verwervende en verwerkende afdelingen kunnen naar behoefte teams worden gevormd waarin analisten (zowel uit de regiobureaus als uit de CIU), *operators* en andere specialisten (bijvoorbeeld uit VI) samenwerken aan één opdracht. Dat kan bijvoorbeeld de ondersteuning van een specifieke crisisbeheersingsoperatie zijn waar de Nederlandse krijgsmacht

aan deelneemt. Denkt u aan het team UNMEE (de VN-vredesoperatie in de Hoorn van Afrika), het team Balkan/Macedonië enzovoort. Maar uiteindelijk moet deze werkwijze in het totale onderzoeksveld van de MID worden toegepast. In teamverband worden ontwikkelingen bekeken, worden indicatoren voor verschillende scenario's vastgesteld en worden onderzoeksvragen geformuleerd voor de verwervende afdelingen. Zo kan zeer doelgericht naar de ontbrekende informatie worden gezocht en kunnen de resultaten direct door het team worden geëvalueerd en verwerkt.

Dan een enkel woord over productiebesturing in het algemeen en vraagsturing in het bijzonder. De capaciteit van de MID is per definitie beperkt: de dienst kan niet ongelimiteerd de hele wereld en alle onderwerpen van militair belang volgen. Het is dus zaak dat

<sup>8</sup> *Current Intelligence*: Current intelligence is recently produced material relating to the current situation and events (STANAG AINTP. 1A).

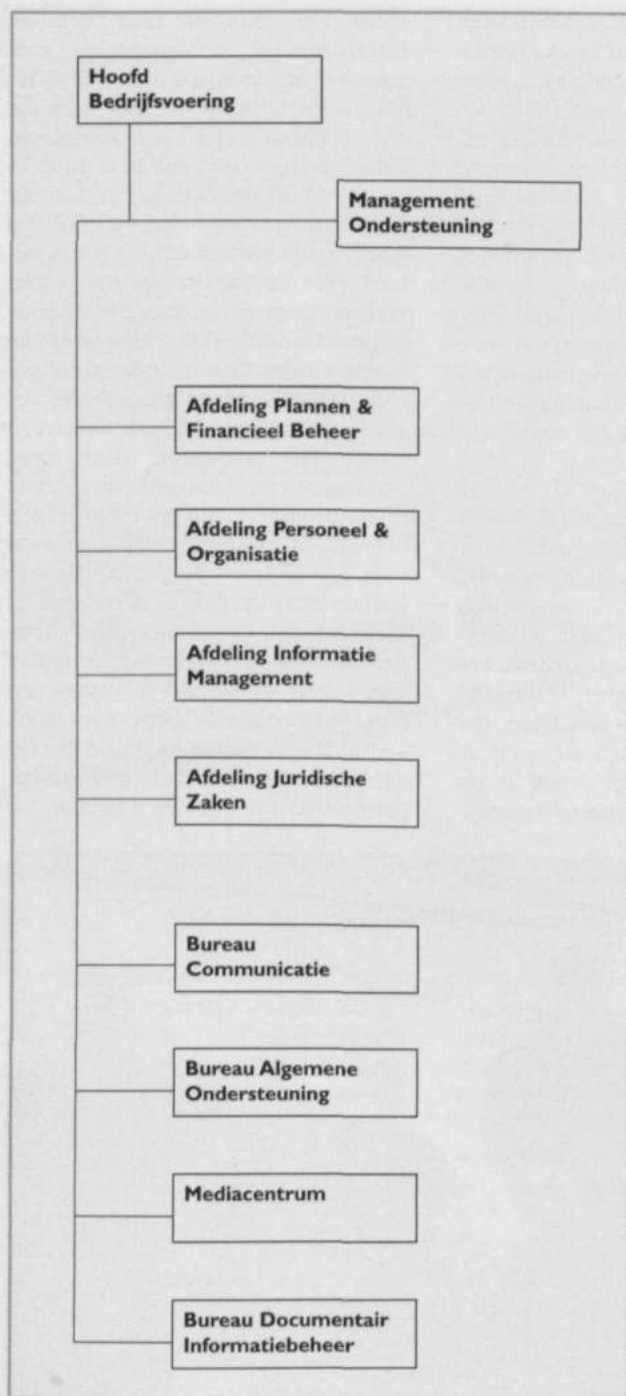
de beschikbare capaciteit zo doeltreffend mogelijk aansluit op de vraag naar inlichtingen. Daartoe maakt de MID jaarlijks in overleg met onze behoeftestellers een werkplan, de zogenoemde Inlichtingen en Veiligheidsbehoefte Defensie (IVD). Zo nauwkeurig mogelijk wordt met elkaar afgesproken waarnaar de MID, met welke prioriteit onderzoek gaat doen en wat voor producten dat zal opleveren. Dat plan wordt in januari door de minister goedgekeurd. De telkens weer optredende spanning tussen vraag en capaciteit wordt opgevangen door indeling van onze onderzoeksactiviteiten in categorieën. De categorisering is bepalend voor de prioriteit, de intensiteit en de mate van diepgang waarmee ontwikkelingen in een bepaald gebied of een thema worden gevolgd. Met andere woorden, het bepaalt de inzet van de bijzondere middelen en de inzet van onze analisten. Uiteraard staan landen en regio's waar Defensie militair is betrokken (of betrokken kan worden) hoog op de prioriteitenlijst.

De stafafdeling Productie is de hoeder van de IVD en stuurt het productieproces aan. Taken zijn onder andere planning en voortgangscntrole van het productieproces, kwaliteitsborging, opleidingsbeleid en relatiebeheer. Voor afstemming met de klanten bij Defensie dragen de vier 'accountmanagers' zorg (liaisonfunctionarissen Defensiestaf, KM, KL en KLu). Zij houden van dag tot dag zicht op de (operationele) activiteiten van de behoeftestellers en op de mate waarin de MID voldoet aan de productieafspraken uit de IVD. Ook zorgen zij ervoor dat zoveel mogelijk voorzien wordt in ad hoc-behoeften. Ten slotte strijken zij waar nodig de – onvermijdelijke – plooitjes glad. Het onderhouden van externe relaties op inlichtingengebied met derden, zoals andere departementen, (buitenlandse) diensten en internationale organisaties, is de taak van het bureau Relatiebeheer. Onderhouden van internationale contacten, sturing van werkbezoeken en management van zogenoemde *requests for information*, zowel uitgaand als inkom-

mend, zijn taken die daar berusten. Internationale samenwerking met andere diensten is, in tegenstelling tot het gangbare beeld dat i&v diensten erg 'op zichzelf zijn', in deze tijd van globalisering, transnationale problematiek en *information overflow*, voor alle diensten een belangrijke en onmisbare informatiebron. Dit resulteert voor de MID in een zeer breed vertakt samenstel van meest bilaterale betrekkingen. Het gaat zowel om uitwisseling van inlichtingen als om technische samenwerking. Vrijwel alle landen, groot en klein, werken zo samen. Als voldoende wordt terug ontvangen voor geleverde diensten is internationale samenwerking een belangrijke *force multiplier*, vooral voor een kleinere partner als de MID (en een klein land als Nederland). Dat klein ook fijn kan zijn is in inlichtingenland evenzeer waar. Nederlanders zijn overal ter wereld te vinden, en hun aanwezigheid roept doorgaans niet al teveel vragen en frictie op. En dat kan in de werkrelatie met grotere partners zo zijn voordelen hebben.



**Uitgezonden militairen kunnen hun taken alleen behoorlijk uitvoeren met goede inlichtingenvoorzieningen**



**Organigram 4**  
**Structuur**  
**hoofdafdeling**  
**Bedrijfsvoering**

### **Hoofdafdeling Bedrijfsvoering**

Ten slotte de hoofdafdeling Bedrijfsvoering (zie organigram 4). Die omvat circa negentig functies. Zoals hierboven al aangegeven is alle capaciteit op het gebied van bedrijfsvoering en

ondersteuning bij de MID uit de (voormalige) productiedelen van de organisatie losgeweekt en gecentraliseerd. Dit bevordert niet alleen een doelmatige inzet en borging van kwaliteit. Het maakt het ook mogelijk om MID-brede concepten voor architectuur en beheer te ontwikkelen en te sturen.

Dat geldt primair voor het informatiemanagement, zoals ICT, ondersteuning van bedrijfsprocessen, documentaire informatievoorziening en archiefvorming. De plaatsvervangend directeur/hoofd Bedrijfsvoering is dan ook de informatiemanager van de MID. Maar denkt u bijvoorbeeld ook aan planning en begroting, en aan financieel en materieelbeheer, alsmede infrastructuur en beveiliging. Op veel van deze essentiële terreinen is de MID nu bezig met een broodnodige inhaalslag. Er wordt goede voortgang gemaakt met verantwoord beheer en met toepassing van nieuwe methoden en technieken. Dat dit ook (soms forse) investeringen vraagt is duidelijk. Maar achterstallig onderhoud is nu eenmaal kostbaar. Een goed plan is echter de basis voor een gezond budget met voldoende investeringsruimte.

In de hoofdafdeling Bedrijfsvoering zijn alle activiteiten samengebracht op het gebied van Personeel en Organisatie, Informatiemanagement, Plannen en Financieel beheer, Documentair Informatiebeheer en Algemene Ondersteuning. Ook de afdeling Juridische Zaken is er ondergebracht. Juridisch advies en toetsing ten behoeve van de directeur MID, maar ook uitvoerende taken zoals het aangeven van randvoorwaarden voor de inrichting van werkprocessen in overeenstemming met de wet, verzoeken om inzage in MID-stukken met een beroep op de Wet Openbaarheid van Bestuur (WOB) en diverse bezwaar- en beroepszaken tegen het handelen van de dienst, behoren tot de verantwoordelijkheden van de juristen. Het Mediacentrum waakt over al het beeldmateriaal van de dienst en faciliteert de *operators* waar nodig en mogelijk.

Voor velen minder aansprekend en niet het eerste waaraan men denkt als het woord 'inlichtingendienst' valt, zijn onderwerpen als documentbeheer en archiefvorming. Voor de kenners van de recente historie van de MID hebben deze onderwerpen echter een bijzondere lading. Gelukkig kan die lading in toenemende mate positief

zijn. Op het gebied van digitalisering van documentbeheer en opslag, alsmede *full text* ontsluiting, is de MID inmiddels binnen Defensie (en ten dele ook daarbuiten) van hekkensluiter, een koploper geworden. Diverse 'pilots' zijn met succes afgerond, onder andere voor de TCBU ('commissie Bakker'). Dit najaar is een project gestart voor dienstbrede invoering. Ook de ordening en ontsluiting van de archieven verloopt tot tevredenheid, ook naar het oordeel van de algemeen rijksarchivaris.

Een nieuw element in de bedrijfsvoering is het bureau Communicatie, van waaruit de interne en externe beeldvorming rond de MID wordt ondersteund. Voor adequate begeleiding van een ingrijpend reorganisatieproces zoals de MID dat nu doormaakt, is dat onontbeerlijk. Zowel aan het eigen personeel als aan de omgeving moet helder worden gemaakt waar de nieuwe dienst voor staat. En ook in het kader van werving van nieuw personeel, hetzij rechtstreeks op de arbeidsmarkt, hetzij intern bij Defensie en de krijgsmacht, is het goed om duidelijk te kunnen maken dat de MID een aantrekkelijke organisatie is om in te werken. *Ingelicht*, het sinds maart 2000 bestaande maandblad van de MID, de kleurrijke *flyer* waarin de dienst wordt beschreven en de brochure inzake veiligheidsonderzoeken, zijn enkele voorbeelden van het communicatieplan van de dienst.

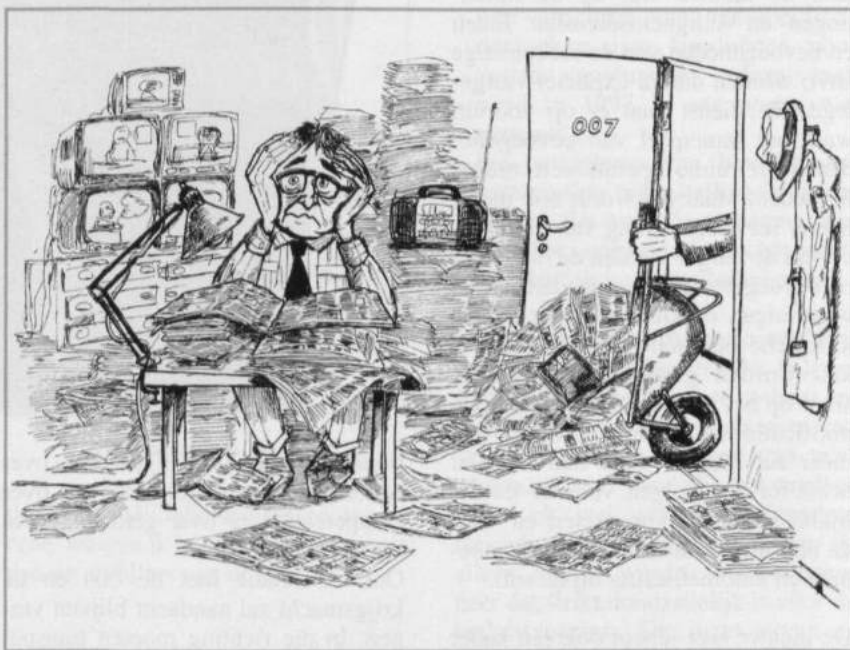
### Veranderingsproces

De 'oude MID' was vele jaren een eilandenrijk; in naam één dienst maar in werkelijkheid versnipperd, moeilijk bestuurbaar, weinig transparant en slecht begrepen. Die tijd ligt nu definitief achter ons. In de nieuwe organisatie en werkwijze richt de dienst zich op zijn kerntaken zoals aangegeven in de wet, en de werkzaamheden die daar niet toe behoren zijn 'ontvlochten'. Doublures zijn uit de organisatie gehaald en de voorwaarden zijn geschapen voor adequate planning en verantwoording.

Dat wil overigens niet zeggen dat er vóór de reorganisatie niet hard en met enthousiasme werd gewerkt bij de MID. Dat was zeker het geval. 'Inlichtingen en veiligheid' is een vak, en de mensen die daarin werken zijn daar trots op. Alleen de samenhang en de richting ontbraken. Een 'informatiefabriek' als de MID moet allereerst zijn klanten kennen en weten wat zij nodig hebben. Vervolgens moeten de verlangde producten volgens een strak en transparant werkproces worden geleverd.

Voor de klant telt alleen de kwaliteit,

De uitvoering ervan is voor de MID in veel opzichten echter een cultuuromslag van formaat. Van geslotenheid en geheimhouding naar zoveel mogelijk openheid en transparantie; van 'onder de pet houden' naar verantwoording afleggen; van voor jezelf werken en op informatie blijven zitten ('geheim!') naar klantgerichtheid; van interne competentiestrijd naar doelgericht en in teamverband samenwerken over de grenzen van de eigen afdeling heen: er waren – en zijn – de nodige tegenstellingen te overbruggen. Om dit te bewerkstelli-



'Open bronnen...'

en daar moet dus op gestuurd worden. Voor de politiek verantwoordelijken en de Nederlandse staatsburgers moet voortdurend duidelijk gemaakt worden dat de dienst zinvol werk doet en daarbij binnen de geldende wettelijke kaders opereert. In die richting is dus transparantie nodig. Bovendien maakt onbekend onbemind. En dat laatste kan een dienst met ambitie zich niet veroorloven. Er is tenslotte een stevig budget nodig (en dat is er ook gekomen).

De logica van dit betoog laat zich zonder moeite in enkele volzinnen

gen is begin 2000 een veranderprogramma voor de MID van start gegaan onder de naam PRISMA (Programma Reorganisatie, Integratie en Stabilisering MID-Afdelingen). De basis onder dit programma is het velen van u bekende INK-model, gericht op integrale kwaliteitsverbetering. In het programma PRISMA zijn ambities vertaald naar doelstellingen en die weer naar concrete projecten. Cultuuromslag en uitvoering van de reorganisatie gaan zo hand in hand. 'Niets is zo praktisch als een goede theorie' is in de wetenschap een gangbare wijsheid. Daarom is een toetsbaar en

meetbaar veranderprogramma een waardevol instrument. Maar het gaat natuurlijk om de uitvoering. En die kost tijd, geld en vooral veel leiderschap, energie en doorzettingsvermogen.

### **Toekomst, slot**

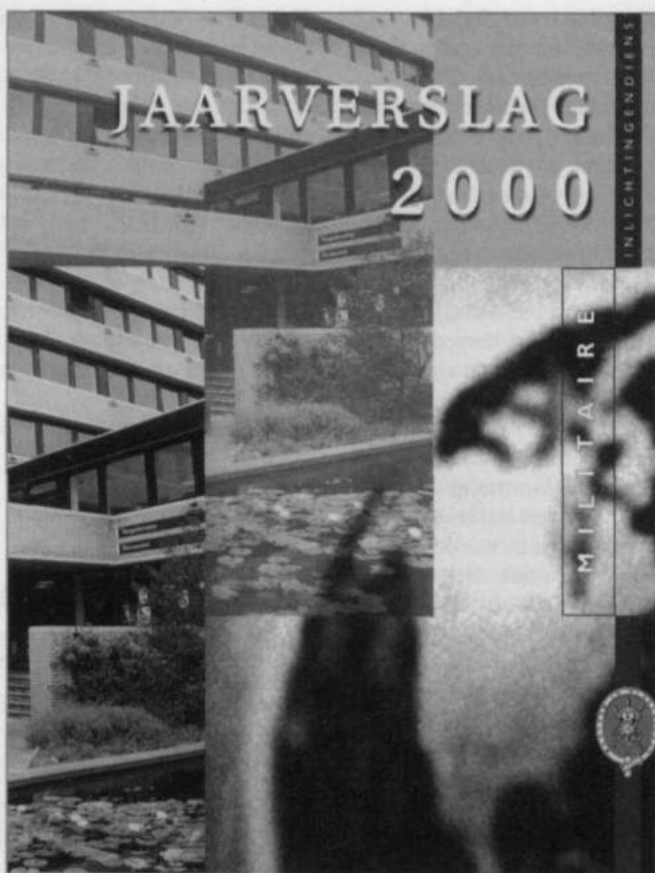
De nabije toekomst van de MID is derhalve glashelder: stug doorgaan met bouwen aan de nieuwe dienst. Deze simpele vaststelling bevat echter wel enkele 'uitdagingen'. Allereerst is daar de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Taken en bevoegdheden van de toekomstige MIVD worden daarin expliciet vastgelegd. De dienst gaat er op vooruit, want het samenstel van bevoegdheden geeft ruime operationele mogelijkheden. Maar het wordt ook moeilijker. Ter bescherming van de privacy van de burger worden de bijzondere bevoegdheden van de dienst met waarborgen omkleed. Zonder in een juridische beschouwing te vervallen, kan worden geconstateerd dat de MIVD op het gebied van lastgevingen, notificatie en verantwoording, nog meer zal moeten doen dan nu. Dat heeft forse gevolgen voor de duidelijkheid van werkprocessen en voor de betrouwbaarheid van documentbeheer en automatisering bij de MID.

De nieuwe wet schept ook een kader voor meer – en wellicht andere – vormen van samenwerking met en tussen de Nederlandse I&V-diensten. Dat geldt zowel voor de verhouding met de BVD (dan AIVD) alsook voor samenwerking met de met opsporing belaste diensten van justitie en politie. Op nationaal niveau binnen wettelijke kaders doelmatigheid nastreven en tegengaan van versnippering van schaarse en kostbare inlichtingenmiddelen, moeten daarbij voorop staan. Discussies over politieke en opera-

tionele verantwoordelijkheden, over wettelijke (on)mogelijkheden, over competenties en over geld liggen in het verschiet.

Ook de relatie met de CDS en de krijgsmacht zal aandacht blijven vragen. In die richting moeten transparantie, voorspelbaarheid en klantgerichtheid worden verbeterd. Voorts zal de komende discussie rond verdere versterking van de positie van de CDS, bij de uitoefening van operationele verantwoordelijkheden, vermoedelijk niet ongemerkt aan de MID voorbijgaan. We zijn tenslotte voor een groot deel 'hofleverancier' van de hoogste militaire baas bij Defensie, maar de klant-leverancieverhouding is in termen van militaire *command and control*, niet altijd even helder.

En *last but certainly not least* moet de consolidatie van de huidige reorganisatie van de MID in een stevig tempo doorgaan en medio 2002 worden afgerond. Een essentiële voorwaarde daarvoor is intensivering van de communicatie in de dienst en versterking van leiderschap op alle niveaus. Te zeer is vernieuwing en verandering nog een zaak van de dienstleiding. Ook dieper in de organisatie moeten leidinggevenden verantwoordelijkheid willen nemen en de dialoog durven aangaan met hun mensen. Alleen op die manier kunnen verandering en cultuuromslag beklijven. Ondertussen blijft tijdens de verbouwing de winkel gewoon open. *Never a dull moment* dus, de komende jaren bij de MID.



# Op weg naar een Algemene Inlichtingen- en Veiligheidsdienst

## De BVD vandaag en morgen

S.J. van Hulst\*

### Inleiding

Sinds mijn aantreden als hoofd van de Binnenlandse Veiligheidsdienst (BVD) in 1997 heb ik verschillende veranderingen meegeemaakt. Zo is de organisatiestructuur van de BVD op een aantal punten gewijzigd en ook op het vlak van de veiligheidsrisico's en de wettelijke kaders hebben zich veranderingen voltrokken. Feitelijk is sprake van een continu veranderingsproces, gericht op de eisen die nu en in de toekomst aan de BVD worden gesteld. Met andere woorden: de BVD van vandaag is ook al voor een deel de BVD van morgen.

In deze bijdrage hoop ik aan te geven langs welke lijnen de BVD van de toekomst nu al zichtbaar wordt. Die BVD zal dan Algemene Inlichtingen- en Veiligheidsdienst (AIVD) heten, wanneer tenminste de Eerste Kamer instemt met het voorstel voor een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten, dat haar deze zomer is voorgelegd. Het wetsvoorstel voorziet onder andere in een naamsverandering van BVD en MID.

Het artikel is als volgt opgebouwd. Na een overzicht van de taken en bevoegdheden volgt de bespreking van de belangrijkste aandachtsvelden van de BVD. Vervolgens wordt ingegaan op de organisatie van de dienst en op enkele aspecten van (politieke) sturing en verantwoording. Daarna komt de nieuwe Wet op de Inlich-



Het logo van de BVD

tingen- en Veiligheidsdiensten aan de orde, waarna ik besluit met een schets van de ambities van de AIVD.

### Taken en bevoegdheden

De Binnenlandse Veiligheidsdienst kan het best worden getypeerd aan de hand van zijn taken en bevoegdheden. Die immers tonen het bijzondere karakter van de BVD.

De drie taken van de Binnenlandse Veiligheidsdienst staan vermeld in de Wet op de Inlichtingen- en Veiligheidsdiensten (1988) en kunnen kortheidshalve als volgt worden omschreven:

– het verzamelen van gegevens over organisaties en personen die door hun doelen of activiteiten aanleiding geven tot het ernstige vermoe-

den dat zij een gevaar vormen voor de samenleving;

- het verrichten van veiligheidsonderzoeken naar kandidaten voor vertrouwensfuncties (deze taak werd in 1997 in een aparte wet geregeld);
- het bevorderen van beveiligingsmaatregelen bij instellingen en bedrijven die van vitaal belang zijn voor het voortbestaan van het maatschappelijk leven in Nederland.

De BVD beschikt over een aantal bijzondere bevoegdheden. De belangrijkste daarvan zijn het volgen en observeren van mensen, de inzet van 'agenten' en het aftappen van telecommunicatie. Voor alle bevoegdheden (ook wel genoemd bijzondere inlichtingenmiddelen) geldt, dat zij alleen mogen worden ingezet wanneer dat strikt noodzakelijk is voor de taakuitvoering. De inzet ervan is afhankelijk van aard en omvang van het veiligheidsrisico dat in het geding is. Lichtere middelen gaan verder voor zwaardere middelen. De bevoegdheden mogen niet worden ingezet bij de uitvoering van veiligheidsonderzoeken en bij de beveiligingsbevorderende taak van de BVD. Een aantal bevoegdheden mag alleen worden gebruikt na ministeriële toestemming.

Bij het verzamelen van gegevens maakt de BVD overigens niet alleen gebruik van bijzondere inlichtingenmiddelen. Het gebruik van open bronnen, al dan niet via internet, maakt, mede met het oog op het beginsel van subsidiariteit, een wezenlijk onderdeel uit van de werkwijze van de BVD.

\* De auteur is hoofd van de Binnenlandse Veiligheidsdienst.



Ook de bevolking speelt een belangrijke rol bij het vergaren van informatie. Burgers attenderen de BVD vaak op zaken die uit oogpunt van de binnenlandse veiligheid van belang zijn. Kenmerkend voor de BVD zijn verder de uitgebreide contacten met buitenlandse inlichtingen- en veiligheidsdiensten. Deze diensten vormen eveneens een zeer waardevolle bron van informatie.

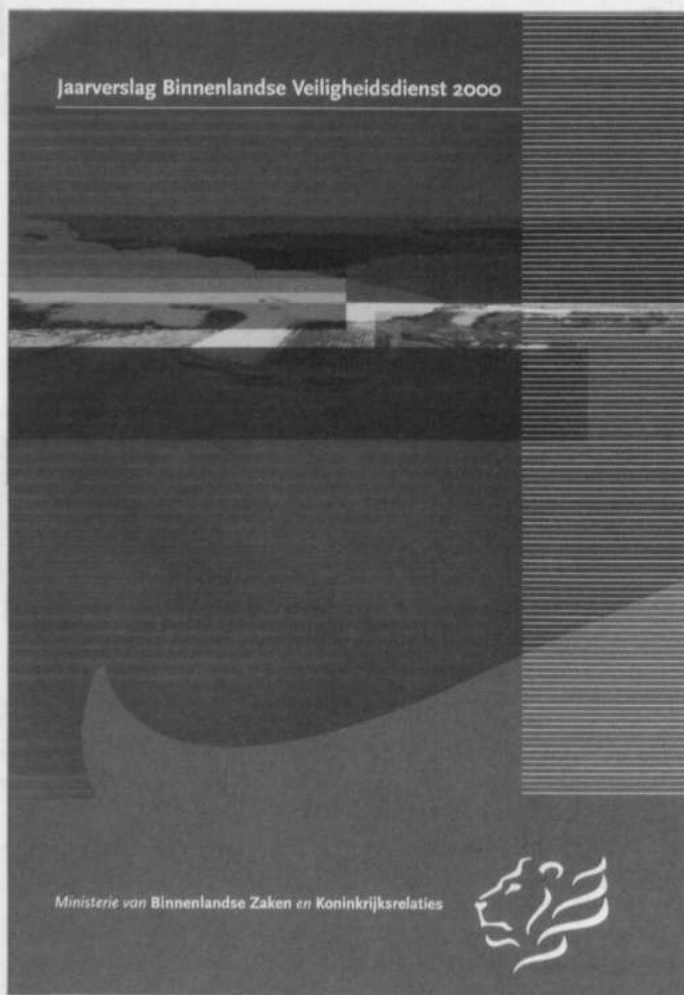
## Aandachtsgebieden

Zo'n veertig jaar lang, in de periode van de Koude Oorlog, bepaalt vooral de dreiging van het communisme in binnen- en buitenland de werkzaamheden van de BVD. In de loop der jaren dienen zich veranderingen aan. Zo komen in de jaren zestig andere dreigingen in beeld in de vorm van nationaal en internationaal terrorisme. Begin jaren tachtig wordt het onderzoek naar de Communistische Partij Nederland (CPN) stopgezet, omdat deze partij geen machtsfactor van betekenis meer vormt. Het einde van de Koude Oorlog betekent echter een drastische verandering in de mondiale verhoudingen. De statische Oost-West-tegenstelling maakt plaats voor een wisselend patroon van spanningen en conflicten, die ook hun weerslag hebben op de veiligheidssituatie in Nederland. Een diversiteit aan aandachtsgebieden voor de BVD is het gevolg. Recentelijk zijn deze aandachtsgebieden binnen de BVD geclusterd in een aantal zogenaamde pijlers. Deze zijn:

### Contra-terrorisme

Met name in het verband van de Europese Unie en de Verenigde Naties levert de BVD een bijdrage aan de strijd tegen het terrorisme. Groeperingen als ETA en IRA vragen om aandacht, maar ook naar radicale islamitische netwerken, zoals die van Osama bin Laden, wordt onderzoek verricht.

Bij de vraag in hoeverre Nederland risico's loopt, is het van belang met enkele factoren rekening te houden.



Nederland ligt op een internationaal logistiek knooppunt, waardoor er sprake is van talrijke vervoersmogelijkheden. Daarbij geniet ons land wereldwijd een zekere faam vanwege onze tolerante houding jegens afwijkende politieke en religieuze opvattingen. In combinatie leiden deze factoren ertoe, dat Nederland ook een relatief geschikte vestigingsplaats is voor personen die (indirecte) steun verlenen aan de anti-westerse strijd van organisaties elders in de wereld. Acties op Nederlands grondgebied zouden dit alleen maar op het spel te zetten en liggen daarom niet direct voor de hand. Gelet op de internationale verplichtingen van Nederland wettigt deze redenering echter geen afwachtende houding van de autoriteiten. (Zie ook de bijdrage over terrorisme.)

### Anti-integratieve tendensen

Nederland ontwikkelt zich tot een multi-etnische samenleving en streeft naar de integratie van uiteenlopende bevolkingsgroepen. Dit integratieproces wordt in een aantal opzichten belemmerd door krachten van binnen en buiten Nederland. Hierbij gaat het met name om import van conflicten uit landen en gebieden van herkomst van allochtone bevolkingsgroepen en om pogingen vanuit die landen – zowel op overheidsniveau als op het vlak van radicale politieke en religieuze organisaties – invloed te blijven uitoefenen op naar elders vertrokken onderdanen.

Beïnvloedingsactiviteiten vanuit landen van herkomst werken niet alleen het van de grond komen van loyaliteit jegens de Nederlandse samenleving tegen, maar maken het voor alloch-

tonen – in ieder geval naar eigen beleving – ook een hachelijke zaak gebruik te maken van in Nederland voor een ieder geldende grondrechten. Een heikel punt is de vraag in hoeverre allochtone groepen hun eigenheid kunnen behouden: eenieder mag rekenen op een respectvolle bejegening, maar deze eigenheid mag niet uitlopen in de schending van (grond)rechten van anderen. Hier dreigt wellicht polarisatie tussen bevolkingsgroepen.

Integratie van allochtonen gaat niet zonder actieve betrokkenheid van de groepen zelf. In dit kader ziet de overheid zich veelvuldig geconfronteerd met verschillende representanten en spreekbuizen van betrokken groepen. De overheid heeft in voorkomende gevallen behoefte aan betrouwbare informatie inzake de status van gesprekspartners, de aard van hun achterban, alsmede de intenties waarmee zij het overleg aangaan.

De BVD draagt bij aan het zichtbaar maken van de tegenkrachten van het integratieproces, zodat overheid en

samenleving beter in staat worden gesteld hiermee adequaat om te gaan.

#### **Gewelddadig politiek activisme**

De BVD maakt een onderscheid tussen gewelddadig politiek activisme en terrorisme. Het eerste is gericht op het aanbrengen van materiële schade, terwijl het tweede vooral is gericht op het maken van slachtoffers. In Nederland komen verschillende vormen van gewelddadig politiek activisme voor. Voorbeelden zijn sommige antimilitaristische acties en gewelddadige acties tegen organisaties en personen die beschuldigd worden van dieren mishandeling. Ook onder de noemer anti-globalisme nemen acties soms gewelddadige vormen aan. Dergelijke vormen van geweld kunnen een ordentelijk proces van democratisch bestuur en besluitvorming doorkruisen en krijgen om die reden de aandacht van de BVD.

#### **Contra-inlichtingen**

Vershillende landen trachten in Nederland langs heimelijke weg

hoogwaardige kennis en goederen te verwerven. Op dit terrein zijn inlichtingendiensten actief uit bijvoorbeeld Rusland en China. Het tegengaan van deze vormen van spionage is van oudsher een taak van de BVD.

Daarnaast zijn er inlichtingendiensten die het gemunt hebben op politieke vluchtelingen in Nederland, zoals die van Irak en Iran. Ook deze inlichtingenactiviteiten kunnen in Nederland uiteraard niet worden getolereerd.

#### **Internationale rechtsorde**

Nederland vormt de vestigingsplaats van tal van internationale organisaties zoals het Joegoslavië Tribunaal, het Internationaal Gerechtshof en het *Scottish Court in the Netherlands* (SCIN) voor het Lockerbieproces. De Nederlandse autoriteiten hebben de taak voorwaarden te scheppen voor het ongehinderd functioneren van deze organen. De BVD speelt daarbij een rol door het leveren van informatie en beveiligingsadvies.

Nederland heeft zich ook verplicht een bijdrage te leveren aan het tegengaan van de verspreiding van massavernietigingswapens en van illegale en politiek ongewenste handel in conventionele wapens. De BVD onderhoudt contacten met het Nederlandse bedrijfsleven om te voorkomen dat ons land betrokken raakt bij de productie van massavernietigingswapens. Daarnaast is de dienst alert op mogelijke ongewenste betrokkenheid van Nederland bij de handel in conventionele wapens.

#### **Integriteit**

Sinds minister Dales van Binnenlandse Zaken in 1992 de integriteit van de overheid aan de orde stelde, heeft ook de BVD hier een taak. Invalshoek daarbij is het voorkomen van systematische inbreuken op het integere functioneren van het openbaar bestuur. Bij een groot aantal overheidsinstanties heeft de BVD onderzoek uitgevoerd naar de wijze waarop de integriteit bevorderd kan worden. Inmiddels worden deze instanties zelf geacht zo'n onderzoek te kunnen uitvoeren, waarbij een handleiding van de BVD



**Het gebouw van de BVD te Leidschendam**

als hulpmiddel kan dienen. Bij de BVD bestaat ook een meldpunt voor aantastingen van de integriteit.

#### **Beveiligingsbevordering**

In het kader van de beveiligingsbevordering neemt de advisering over informatiebeveiliging, met name waar het gaat om staatsgeheimen en andere kwetsbare informatie, een belangrijke plaats in. Daarbij moet ingespeeld worden op de toenemende afhankelijkheid van kwetsbare informatie- en communicatietechnologie.

In het kader van de bescherming van vitale bedrijven, zoals bijvoorbeeld de luchthaven Schiphol, geeft de BVD advies over te nemen beveiligingsmaatregelen.

#### **Veiligheidsonderzoeken**

In Nederland bestaan circa 66.000 vertrouwensfuncties. Dat zijn functies bij overheid en bedrijven die de mogelijkheid bieden de veiligheid of andere gewichtige belangen van de staat schade toe te brengen. Jaarlijks verricht de BVD een groot aantal veiligheidsonderzoeken naar de kandidaten voor deze vertrouwensfuncties. Binnenkort wordt het aantal vertrouwensfuncties uitgebreid met de aanwijzing van vertrouwensfuncties bij de politie.

Naast de hier genoemde min of meer reguliere aandachtsgebieden, speelt de actualiteit een belangrijke rol. De beveiligingsaspecten van het Lockerbieproces, EK 2000 en gewelddadige acties van Molukkers zijn voorbeelden van recente onderwerpen, waarbij betrokkenheid van de BVD noodzakelijk bleek. Op deze momenten moet de dienst slagvaardig kunnen inspelen op de ontwikkelingen die zich aandienen.

#### **Organisatie**

De organisatie van de BVD is begin jaren negentig van de vorige eeuw ingrijpend gewijzigd. De structuur die ten tijde van de Koude Oorlog functioneel was, voldeed niet meer in de nieuwe situatie. In het werkproces van de twee directies die met het ver-

zamelen van gegevens zijn belast (de eerste taak van de BVD) werd het teamconcept geïntroduceerd. De teams bestaan daarbij uit mensen met verschillende functies (zoals onderzoekers, bewerkers, analisten, en operateurs), die hun thuisbasis hebben in verschillende afdelingen (de afdeling onderzoek, bewerking en analyse en dergelijke). De teams kennen een projectmatige werkwijze.

Inmiddels is gebleken dat deze matrixstructuur niet helemaal voldoet. Vele teams bleken een langer leven beschoren dan aanvankelijk werd gedacht. Daarom is gekozen de afdelingen op te heffen en de mensen, met hun verschillende functies, permanent in een team onder te brengen. Dit met handhaving van de mogelijkheid om (tijdelijk) ook aan een ander team deel te nemen. Daarmee is een nieuw evenwicht gevonden. De twee genoemde directies kennen naast de operationele teams, ook allebei een afdeling Beleid en Expertise.

Bij deze reorganisatie, die in 1999 zijn beslag kreeg, zijn de werkzaamheden in het kader van de beveiligingsbevordering en de veiligheidsonderzoeken (de tweede en derde taak) samengebracht in een aparte directie. Sinds 1 januari 2001 maakt ook het Nationaal Bureau Verbindingsbeveiliging deel uit van de BVD. Dit bureau vervult eveneens een taak op het vlak van de beveiligingsbevordering.

#### **Sturing en verantwoording**

De minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de Binnenlandse Veiligheidsdienst. In de Ministeriële Commissie voor de Inlichtingen- en Veiligheidsdiensten (MICIV), onder voorzitterschap van de minister-president, wordt het beleid van BVD en MID op elkaar afgestemd. De ambtelijke voorbereiding vindt plaats in het Comité Verenigde Inlichtingendiensten Nederland (CVIN), waarin ook

hoofd BVD en directeur MID zitting hebben.

Naast het plenaire overleg met de Tweede Kamer over de BVD, bijvoorbeeld bij de begrotingsbehandeling of de bespreking van het jaarverslag, vindt regelmatig vertrouwelijk overleg plaats met de commissie voor de Inlichtingen- en Veiligheidsdiensten. Deze bestaat uit de fractievoorzitters van de vier grootste politieke partijen. Op aandringen van de Kamer zal de controle op het werk van de diensten in de toekomst worden uitgebreid (zie hierna).

De afgelopen tien jaar is een grotere mate van openheid ontstaan rond het werk van de BVD. Vanuit het besef dat in een democratische samenleving ook een veiligheidsdienst zich voortdurend moet verantwoorden, is de informatieverstrekking sterk verbeterd. Zo wordt sinds tien jaar een jaarverslag uitgegeven, waarin alle aandachtsgebieden van de BVD aan bod komen en tevens een overzicht wordt gegeven van de algemene ontwikkelingen op het gebied van de binnenlandse veiligheid. Ook buiten het jaarverslag wordt waar mogelijk informatie verstrekt over het doen en laten van de BVD. Bijvoorbeeld door het uitgeven van publicaties over specifieke onderwerpen. Op internet is via de website van het ministerie van Binnenlandse zaken en Koninkrijksrelaties ([www.minbzk.nl](http://www.minbzk.nl)) de nodige informatie over de BVD te verkrijgen. Op grond van de Wet Openbaarheid van Bestuur worden jaarlijks tientallen verzoeken om inzage in persoonsdossiers behandeld. Dit alles laat onverlet dat een zekere mate van geheimhouding, met name waar het gaat om bronnen en werkwijzen, noodzakelijk is voor het goed functioneren van de dienst.

#### **De Algemene Inlichtingen- en Veiligheidsdienst**

In juli 2001 is de Tweede Kamer akkoord gegaan met het voorstel voor een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Met deze wet

wordt beoogd de transparantie rond de BVD (en de MID) te vergroten en de controle te versterken. Tevens zijn de taken en bevoegdheden aangepast aan de eisen van deze tijd. Wanneer de nieuwe wet door de Eerste Kamer is aanvaard, krijgen BVD en MID een nieuwe naam, namelijk Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Hieronder volgen in kort bestek de belangrijkste wijzigingen die de nieuwe wet voor de BVD met zich meebrengt.

De bijzondere bevoegdheden worden expliciet in een wet geregeld. Dat wil zeggen: wanneer een bevoegdheid niet in de wet is opgenomen, kan deze niet worden uitgeoefend. De nieuwe wet kent de AIVD daarnaast een enkele nieuwe bevoegdheid toe. Zo kan de AIVD bijvoorbeeld brieven openen als de rechtbank Den Haag daartoe toestemming heeft gegeven en wordt het mogelijk gemaakt kennis te nemen van informatie in computerbestanden. Voor veel bijzondere bevoegdheden geldt, dat ze pas mogen worden uitgeoefend na toestemming van de minister van Binnenlandse Zaken en Koninkrijksrelaties.

Een andere belangrijke wijziging is de invoering van een notificatieplicht. Dat wil zeggen dat de persoon jegens wie een bijzondere bevoegdheid is gebruikt die inbreuk maakt op de in artikel 12 (huisrecht) en artikel 13 (brief- en telefoongegeheim) van de Grondwet genoemde grondrechten, hierover na vijf jaar wordt geïnformeerd.

Ter versterking van de controle op het werk van de inlichtingen- en veiligheidsdiensten wordt een onafhankelijke Commissie van Toezicht ingesteld bestaande uit drie leden. De leden zullen op voordracht van de Tweede Kamer bij koninklijk besluit worden benoemd.

De AIVD heeft – naast de taken van de huidige BVD – een nieuwe taak, namelijk het verrichten van onderzoek betreffende andere landen. De onder-

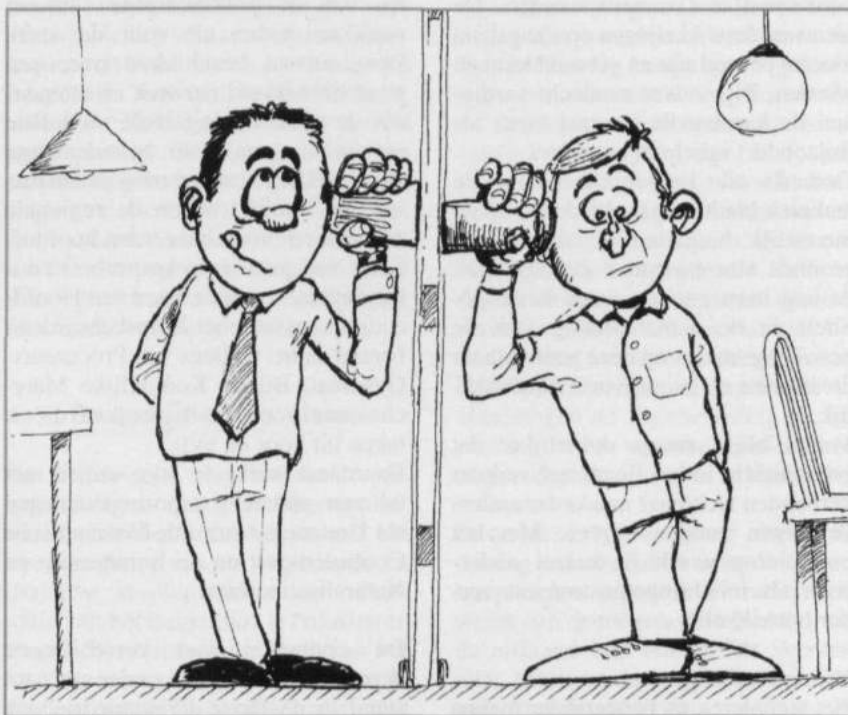
werpen van het onderzoek worden door de minister-president in overeenstemming met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie aangewezen.

### Ambities

De omvorming van Binnenlandse Veiligheidsdienst naar Algemene Inlichtingen- en Veiligheidsdienst krijgt naar verwachting in 2002 zijn beslag. De AIVD staat, net als de BVD,

werkerterrein van de dienst. Ontwikkelingen in en rond potentiële conflict-haarden in de wereld, alsmede in en rond staten en regio's die zich kenmerken door instabiliteit en non-transparantie, zullen in het bijzonder de aandacht krijgen. De nadruk in de inlichtingentaak zal, vanwege de positie van Nederland en zijn politieke ambities, liggen bij analytische activiteiten eerder dan bij grootschalige risicovolle operaties.

De combinatie van de inlichtingen- en veiligheidstaak in een dienst komt in weinig landen voor. De inbedding



'Afluisteren...'

voor de opgave aantastingen van de nationale veiligheid tijdig in beeld te brengen en anderen in staat te stellen de nodige maatregelen te treffen. Centraal in de verdere ontwikkeling van de AIVD, staat de ambitie zowel qua kennis als qua kunde een betrouwbare en gezaghebbende autoriteit op het terrein van de nationale veiligheid te zijn. Integriteit en professionaliteit staan daarbij hoog in het vaandel.

### Inlichtingentaak

De nieuwe inlichtingentaak buitenland betekent een verbreding van het

van de nieuwe, meer offensief gerichte taak in een vanoudsher defensief ingestelde veiligheidsdienst, zal de nodige aandacht vragen.

### Antenne

Veiligheidsrisico's veranderen – mede onder invloed van technologische ontwikkelingen – sneller van karakter en zijn minder zichtbaar, minder voorspelbaar en meer grensoverschrijdend geworden. Het is daarom van belang dat de AIVD kan beschikken over een goed ontwikkelde antenne voor ontwikkelingen in de

(internationale) samenleving (met gevoel voor *sense of emergency* en *sense of urgency*) en beargumenteerd heldere prioriteiten kan stellen. Hiervoor is het noodzakelijk de strategie- en scanfunctie van de AIVD (verder) te ontwikkelen en uit te bouwen.

#### Inlichtingenmiddelen

De snelle technologische veranderingen dwingen tot voortdurende alertheid ten aanzien van de effectiviteit van het arsenaal van inlichtingenmiddelen. Waar nodig dient aangepast en vernieuwd te (kunnen) worden. De nieuwste ontwikkelingen op ICT-gebied moeten bekend zijn en gebruikt kunnen worden. Bijzondere aandacht verdienen de kansen die internet biedt als (bijzonder) inlichtingenmiddel.

Ondanks alle mogelijkheden die de techniek biedt en gaat bieden, blijven menselijk handelen en menselijke bronnen van essentieel belang. Juist de nog immer toenemende heterogeniteit in de samenstelling van de bevolking, maakt op deze punten meer creativiteit en inventiviteit noodzakelijk.

Voorts blijkt steeds duidelijker dat goed inzicht in het financieel verkeer verbanden zichtbaar maakt die anders verborgen zouden blijven. Met het oog hierop wordt financieel onderzoek als inlichtinginstrument verder ontwikkeld.

#### Samenwerking

Het signaleren en beheersbaar maken van complexe veiligheidsrisico's maakt samenwerking met andere instanties die bij de zorg voor veiligheid een rol spelen, steeds meer noodzakelijk. De diensten, waarmee ook in de toekomst nauwe samenwerking geboden blijft, zijn met name de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de politie en de

Koninklijke Marechaussee. Met de MIVD vindt onder meer samenwerking plaats op het vlak van de contra-inlichtingen en het tegengaan van de verspreiding van massavernietigingswapens. Daarnaast wordt de inbreng van de diensten in tal van overlegvormen op elkaar afgestemd, zoals in het verband van NAVO en West-Europese Unie. De inlichtingentaak van beide diensten zal leiden tot verdere intensivering van de samenwerking.

Bij de politie voeren de medewerkers van de Regionale Inlichtingendiensten van de politiekorpsen (RID-en) werkzaamheden uit voor de AIVD. Deze RID-en beschikken over een goed ontwikkeld netwerk en attenderen de AIVD op regionale en lokale ontwikkelingen. Over beleidsmatige vraagstukken vindt overleg plaats tussen het hoofd BVD en de regionale driehoeken (korpsbeheerder, hoofdofficier van justitie en korpschef) en – incidenteel – met de Raad van Hoofddirecties, het Korpsbeheerdersberaad en het College van Procureurs-Generaal. Bij de Koninklijke Marechaussee voert de bijzondere dienst taken uit voor de BVD.

Daarnaast werkt de AIVD samen met tal van andere (opsporings)diensten als Douane en FIOD, de Economische Controledienst en de Immigratie- en Naturalisatiedienst.

De contacten met verschillende departementen komen onder meer tot stand in de Grote Evaluatiedriehoek en de Technische Evaluatiecommissie. Dit zijn interdepartementale adviesorganen voor beveiligings- en bewakingsaangelegenheden waarvoor de rijksoverheid de verantwoordelijkheid draagt. Daarnaast vindt over tal van onderwerpen overleg plaats met de ministeries van Economische Zaken, Buitenlandse Zaken, Justitie en

Verkeer en Waterstaat. De inlichtingentaak buitenland als nieuw onderdeel van het takenpakket van de AIVD, maakt contacten met meerdere departementen gewenst en geeft bestaande relaties een nieuwe dimensie.

Binnen het Koninkrijk werkt de AIVD al samen met de veiligheidsdiensten van Aruba en de Nederlandse Antillen. De basis hiervoor is de verplichting tot wederzijdse bijstand in het Statuut van het Koninkrijk. Ten slotte maakt de AIVD deel uit van de internationale wereld van inlichtingen- en veiligheidsdiensten. Binnen Europa bestaan verschillende samenwerkingsverbanden, evenals binnen NAVO en WEU-verband. Daarnaast onderhoudt de AIVD, vanwege de voortgaande internationalisering van het werk, contact met een toenemend aantal buitenlandse diensten in verschillende delen van de wereld. In Washington, Caracas, Amman, Singapore en Moskou zijn AIVD-liaisons gestationeerd. Mede met het oog op de nieuwe inlichtingentaak is het streven erop gericht de contacten en vormen van samenwerking met collegadiensten te intensiveren.

#### Slot

De AIVD zal het werk van de BVD voortzetten. De nieuwe wet biedt de AIVD een duidelijk omschreven geheel van taken en bevoegdheden en voorziet als pendant in een afgewogen stelsel van sturing en verantwoording. Daarmee wordt recht gedaan aan terechte eisen van democratische legitimiteit en kan de komende periode aan de grote variëteit van hedendaagse risico's voor de nationale veiligheid naar verwachting adequaat het hoofd worden geboden.

# Strategische inlichtingen en de Verenigde Naties

F.E. van Kappen – generaal-majoor der mariniers b.d.\*

Toen mij werd gevraagd een artikel te schrijven over het onderwerp 'Inlichtingen en de Verenigde Naties', heb ik even geaarzeld, omdat ik gedurende mijn periode als militair adviseur van de secretaris-generaal van de VN vaak met dit onderwerp heb geworsteld en niet altijd geheel onbeschadigd uit de strijd ben gekomen.

Het is een complex en controversieel onderwerp en de verleiding is dan ook groot om het onderwerp te vermijden. Niet alleen omdat het onplezierige herinneringen oproept, maar ook omdat ik nooit het volle zicht op dit onderwerp heb verkregen. Hoewel er vele manieren zijn om het onderwerp te benaderen, is en blijft het een exercitie die veel weg heeft van het ontwarren van een Gordiaanse knoop. Het gevaar is dan ook aanwezig dat de lezer na afloop blijft zitten met meer vragen dan antwoorden. Het feit dat u dit artikel nu leest, houdt in dat ik in ieder geval een poging wil wagen om mijn verwarring over dit onderwerp met u te delen.

De verwarring begint eigenlijk al met het feit dat er binnen het Secretariaat van de VN zeer verschillend over dit onderwerp wordt gedacht. Ook de lidstaten van de VN hebben geen eenduidige visie en bovendien wordt de discussie vertroebeld door definitieproblemen; wat door de een wordt aan-

gemerkt als het verzamelen van inlichtingen, wordt door de ander gekwalificeerd als het verzamelen van informatie; wat voor de een valt onder het hoofdstuk strategische inlichtingen, valt voor de ander onder het hoofdstuk spionage. Bovendien wordt het onderscheid tussen strategische inlichtingen en tactische inlichtingen niet door iedereen begrepen en diegenen die het wel begrijpen, verschillen van mening over waar de scheidslijn precies moet worden getrokken.

## De traditionele visie

De traditionele visie binnen de VN-organisatie is dat inlichtingenactiviteiten zich slecht verdragen met het open karakter van de organisatie en derhalve absoluut taboe zijn. Deze visie valt het duidelijkst te beluisteren binnen het humanitaire deel van het VN-systeem zoals bijvoorbeeld UNHCR, WFP en UNICEF. Dit heeft te maken met het feit dat de humanitaire VN-organisaties voor hun operaties geen verantwoording verschuldigd zijn aan de Veiligheidsraad.

Voor het Secretariaat van de VN in New York ligt dit uiteraard anders. De twee belangrijkste departementen binnen het Secretariaat, het *Department of Peacekeeping Operations* (DPKO) en het *Department of Political Affairs* (DPA) zijn direct betrokken bij het voorbereiden en uitvoeren van vredesoperaties en zijn hiervoor verantwoording schuldig aan de Veiligheidsraad.

Hoewel ook het Secretariaat van oudsher het uitgangspunt hanteerde

dat het verzamelen van inlichtingen ter ondersteuning van vredesoperaties ongewenst was, zijn velen binnen het Secretariaat de laatste jaren geleidelijk aan tot de conclusie gekomen dat dit misschien toch wel eens noodzakelijk zou kunnen zijn. Ik formuleer dit zo omslachtig, omdat men deze conclusie slechts met grote aarzeling heeft getrokken en deze niet door iedereen wordt gedeeld. Zelfs op dit moment zijn er nog veel functionarissen binnen het Secretariaat die vasthouden aan de traditionele visie, dat het verzamelen en het gebruik van inlichtingen ter voorbereiding en uitvoering van vredesoperaties een ongeoorloofde activiteit is binnen het VN-systeem.

Door deze laatste groep wordt de omslag in het denken over dit onderwerp als iets negatiefs ervaren en verweten aan de toegenomen invloed van de militaire staf binnen het Secretariaat. DPKO, en dan met name de militaire staf binnen DPKO, heeft steeds gewezen op de harde lessen die geleerd zijn op dit gebied tijdens de operaties in Bosnië, Somalië en Rwanda, waar overduidelijk is gebleken dat interventie in dit soort complexe interne conflicten, zonder te beschikken over goede strategische inlichtingen, uiterst riskant is.

## De gewijzigde aard van internationale conflicten

Hiermee zijn we meteen aangeland bij een feit dat in dit kader van groot belang is. De aard van de conflicten waarmee de VN te maken heeft, is

\* De auteur was van 1995 tot 1998 militair adviseur van de secretaris-generaal van de Verenigde Naties en Director Planning Division in the Department of Peacekeeping Operations van de VN.

sedert de val van de Berlijnse Muur ingrijpend veranderd. Gedurende de Koude Oorlog had de VN voornamelijk te maken met conflicten tussen staten; sedert het einde van de Koude Oorlog heeft de VN echter voornamelijk te maken met interne conflicten; met burgeroorlogen dus en met *failed states*.

Wil de internationale gemeenschap dit soort operaties tot een goed einde brengen, dan zal men de oorzaken van de problemen moeten aanpakken. De oplossing van deze problemen vereist een multidisciplinaire aanpak en omvat een groot aantal uiteenlopende activiteiten zoals het weer opstarten van de economie, het vinden van oplossingen voor kwesties van religieuze en/of etnische aard, het herstel van de rechtsorde etc. De militaire operatie kan slechts de veiligheidsparaplu verschaffen waaronder dit echte vredesproces kan plaatsvinden. Dit proces is uiterst complex en civiel van karakter en wordt uitgevoerd door een groot aantal instanties en organisaties. Het probleem is echter dat niemand echt de leiding heeft en het proces derhalve vaak ongestructureerd en ongecoördineerd verloopt.

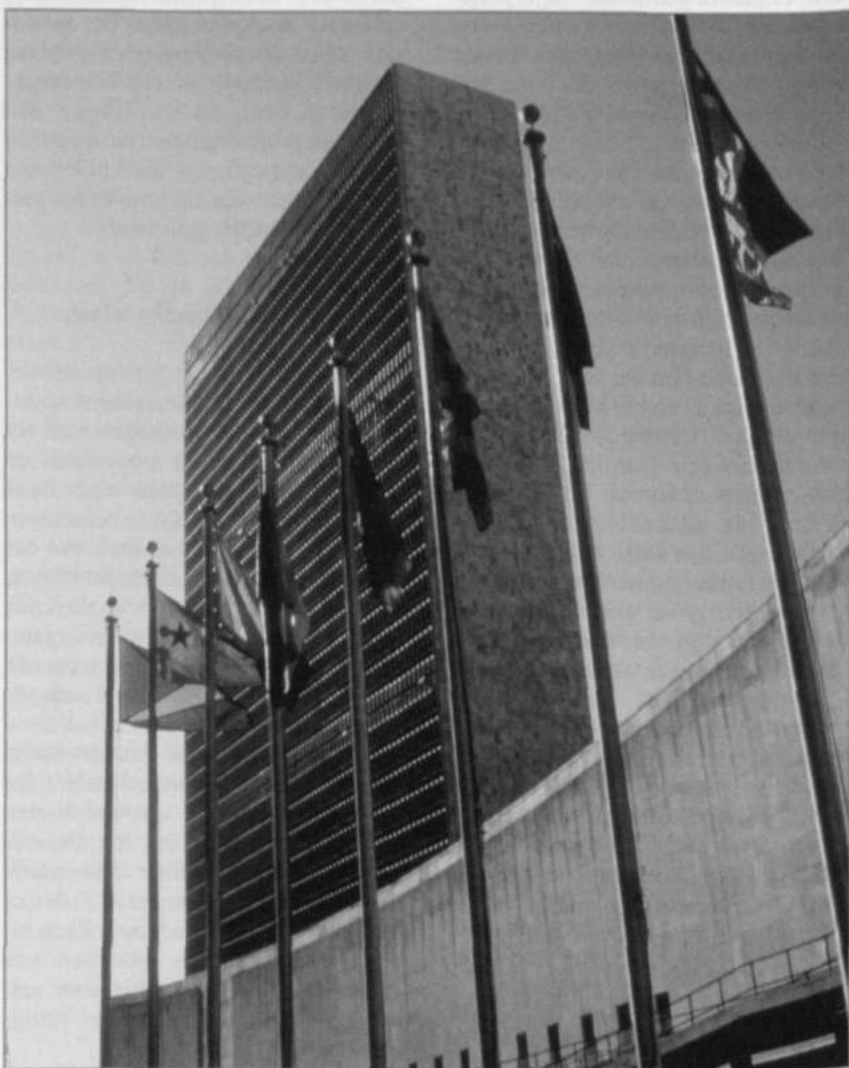
De verleiding is groot om dit onderwerp verder uit te diepen, omdat het zo belangrijk is, maar dat zou ons te ver wegvoeren van het onderwerp van deze bijdrage. Wel is het van belang om in dit kader te constateren dat het bij dit soort *complex emergencies* belangrijk is om een totale strategie te ontwerpen voor de oplossing van het conflict. De militaire bijdrage is slechts een onderdeel van deze totale strategie. Het is dus van groot belang om over goede strategische inlichtingen te kunnen beschikken op velerlei gebied. Het gaat daarbij om politieke, diplomatieke, economische en militaire informatie die besluitvorming op het hoogste niveau mogelijk moet maken. Ik ben er persoonlijk van overtuigd dat het gebrek aan strategische inlichtingen een belangrijke oorzaak is geweest voor het falen van een aantal VN-operaties.

### Strategische inlichtingen

Het Secretariaat van de VN is op het gebied van strategische inlichtingen in belangrijke mate afhankelijk van de vijf permanente leden van de Veiligheidsraad. Datgene dat op dit gebied wordt aangereikt, is niet altijd politiek neutraal, om het maar eens voorzichtig uit te drukken. Ik heb zelf het vermoeden dat deze afhankelijkheid van het Secretariaat de permanente leden van de Veiligheidsraad wel goed uitkomt en er derhalve weinig behoefte is om de afhankelijkheid op dit gebied te verminderen. De oplossing die na lang aarzelen is gekozen om toch invulling te geven

aan de herhaalde en aantoonbare wens, van met name de militaire staf, om te kunnen beschikken over inlichtingen ter voorbereiding en ondersteuning van operaties, weerspiegelt zowel de interne aarzeling over dit onderwerp binnen het Secretariaat, als de terughoudendheid van de permanente leden van de Veiligheidsraad om aan deze wens tegemoet te komen.

Het *Situation Center* in New York werd na lang aarzelen uitgebreid met een aparte afdeling waar de vijf permanente leden van de Veiligheidsraad elk een inlichtingenfunctionaris hebben geplaatst. Vragen en wensen op



Gebouw van het vn-hoofdkwartier in New York (Bron: abc-press)

inlichtingengebied kunnen door DPKO en anderen binnen het Secretariaat, aan deze functionarissen worden voorgelegd. Vervolgens worden deze vragen en wensen door deze functionarissen voorgelegd aan de inlichtingendiensten van het land dat zij vertegenwoordigen. Eventuele antwoorden worden wederom via deze functionarissen teruggekoppeld naar het Secretariaat.

De aansturing van deze afdeling was volslagen onduidelijk en veroorzaakte voortdurend wrijving en onmin binnen DPKO en elders binnen het Secretariaat. Bovendien werd de structuur en het product van deze onbestuurde afdeling niet alleen door veel lidstaten van de VN, maar ook door veel functionarissen binnen het Secretariaat, met groot wantrouwen bezien. Dit was overigens niet zonder reden.

Ik heb meermalen het vermoeden gehad dat de producten bedoeld waren om de VN, of althans DPKO, te manipuleren. Tijdens de humanitaire crisis in het toenmalige Oost-Zaire, waren de inlichtingen die via deze afdeling werden verstrekt over het lot, de toestand en het aantal vluchtelingen, een duidelijke afspiegeling van de positie die het desbetreffende lid van de permanente vijf innam ten aanzien van de te volgen koers. Was het land voor ingrijpen, dan was er sprake van veel vluchtelingen en hun toestand was erbarmelijk; was het land tegen ingrijpen, dan viel het aantal vluchtelingen erg mee en was hun toestand redelijk. Het aantal vluchtelingen was verworden tot het onderwerp voor een fikse politieke ruzie. Een aantal landen ging zelfs zover dat men op eigen houtje verkenningsvluchten liet uitvoeren boven Oost-Zaire om het aantal vluchtelingen te kunnen vaststellen. Het was al bij al een beschamende vertoning. Zo zijn er veel voorbeelden te geven, maar dat zou te veel tekst in beslag nemen. Ook ben ik er persoonlijk van overtuigd dat in een aantal gevallen cruciale informatie willens en wetens niet werd doorgegeven aan de VN, omdat dat blijkbaar politiek gezien niet goed uitkwam. Het is geen geheim dat de

vs actief betrokken zijn geweest bij het trainen van het Kroatische leger voor het Kraïna-offensief. Dit gebeurde door tussenkomst van een zogenoemd *Private Military Company*, die gevestigd is in Washington en handelde in opdracht van de autoriteiten in Washington. Merkwaardigerwijs heeft DPKO nimmer een officiële waarschuwing ontvangen van de vs dat het Kroatische leger een offensief zou beginnen. Een offensief dat geleid heeft tot een aantal gruwelijke moord-

binnen mijn staf belast was met de operatie. Ook kwam het voor dat de (burger)functionaris in DPKO, die belast was met de politieke aspecten van een missie, niet mocht worden ingelicht. Het werken werd op die manier erg moeilijk en de onderlinge samenwerking werd er niet beter op.

Ten tijde van de missie van de VN in Oost-Slavonië (UNTAES) deed zich een soortgelijk probleem voor. Aangezien de *Force Commander* (FC) en het



Dezelfde vlag, verschillende visies (Bron: foto Hennie Keeris)

partijen onder de burgerbevolking in de Kraïna en waarbij ook slachtoffers te betreuren waren aan de kant van UNPROFOR.

Een ander probleem met de gekozen constructie was dat de aangeleverde inlichtingenproducten soms mondeling werden verstrekt en dan vaak ook nog met de mededeling, dat deze informatie slechts bekend mocht worden gesteld aan een beperkt aantal met naam genoemde functionarissen en aan niemand anders. Ook mocht de informatie vaak niet op schrift worden gesteld. Ik heb het meerdere malen meegemaakt dat ik de informatie niet mocht delen met mijn *deputy* of met de desbetreffende officier die

grootste deel van de staf te velde werden geleverd door België, was de NAVO bereid om zowel strategische als tactische inlichtingen te verstrekken aan UNTAES. Een bijkomende voorwaarde was echter, dat de sectie 2 van UNTAES uitsluitend bemand mocht worden met officieren die afkomstig waren uit NAVO-landen. Aangezien België het enige NAVO-land was dat aan deze operatie deelnam, betekende dit dat de sectie 2 uitsluitend met Belgische officieren mocht worden bemand. Dit gaf aanleiding tot grote woede en frustratie bij de grootste troepenleveranciers voor de operatie (Rusland, Pakistan, Jordanië en de Oekraïne). Door België is toen druk uitgeoefend op Nederland om deel te nemen aan



de operatie. Nederland voelde daar niets voor, maar heeft uiteindelijk, om België tegemoet te komen, een aantal stafofficieren geleverd om samen met de Belgen de sectie 2 te bemannen, zodat het inlichtingenwerk in ieder geval geen exclusief Belgische aangelegenheid zou zijn.

Het feit dat de FC zijn Russische *deputy*, en de officieren in zijn staf die afkomstig waren uit *niet-NAVO*-landen, geen inzage mocht geven van de door NAVO aangeleverde informatie, heeft voortdurend geleid tot spanningen in de staf van UNTAES. Uiteraard

### Het glazen huis

Ik begrijp overigens best dat de terughoudendheid van landen om inlichtingen te delen met DPKO, wordt veroorzaakt door het feit dat het hele Secretariaat zo lek is als een mandje. Een van de inlichtingenfunctionarissen verontschuldigde zich eens tegenover mij met de opmerking:

*if you enter this building and even think about something, it is known in 185 different capitals in the world within one hour.*



**Strategische mobiliteit is nodig** (Bron: foto Hennie Keeris)

leverde dit ook de nodige problemen op in DPKO in New York. Hoewel de NAVO in die dagen op roulatiebasis een liaisonofficier leverde in het VN-hoofdkwartier in New York, werd de gehele constructie met grote frustratie en ingehouden woede bezien. Dit gold zowel voor een aantal functionarissen binnen DPKO als voor diverse ambassadeurs in New York van de landen die troepen leverden voor UNTAES. Ik heb er een hoop kopzorgen over gehad en de samenwerking binnen DPKO, maar ook daarbuiten, heeft er onder geleden.

In datzelfde gesprek werd meerdere malen gesuggereerd dat een aantal functionarissen in DPKO actief betrokken was bij het verzamelen van inlichtingen voor diverse inlichtingendiensten. Ik heb daar zelf geen enkel bewijs voor, maar de perceptie is vaak belangrijker dan de waarheid. Vaak is het ook zo dat bepaalde inlichtingen niet worden gedeeld, omdat men een terechte angst koestert dat de bron kan worden gecompromitteerd of dat er conclusies getrokken kunnen worden over de technische capaciteit van bepaalde appara-

tuur. De middelmatige kwaliteit van de satellietfoto's van de massagraven na de val van Srebrenica, die door de VS aan de VN ter hand werden gesteld, heeft waarschijnlijk iets te maken met deze laatste overweging.

Een andere factor die een rol speelt in het geheel, is dat veel troepenleverende landen hun eigen inlichtingenactiviteiten opvoeren in het desbetreffende operatiegebied en die gebruiken om hun eigen analyse van de toestand te maken. Best te begrijpen, maar het beeld wordt er niet overzichtelijker door.

Een voorbeeld van dit verschijnsel was het opereren van SAS-eenheden van het Verenigd Koninkrijk in Bosnië ten tijde van UNPROFOR. Weer een ander voorbeeld was de inlichtingenactiviteit die door de VS ten tijde van de VN-operatie in Somalië werd bedreven. Het zal duidelijk zijn dat de inlichtingen die tijdens deze activiteiten werden verzameld, rechtstreeks aan respectievelijk Londen en Washington werden gerapporteerd en niet aan de VN in New York.

Het feit dat DPKO in New York toch vaak op de hoogte was van deze activiteiten, heeft te maken met inlichtingenactiviteiten van weer *andere* lidstaten in het operatiegebied die DPKO, om hun moverende redenen hierover (uiteraard informeel) informeerden. Het is echt oppassen geblazen in dat soort situaties; voordat je het weet wordt er door iemand een inschattingfout gemaakt bij dit complexe schaduwspel en gaat er iets afschuwelijk mis.

Een voorbeeld van een dergelijke situatie was het incident in Ruanda waar een massale slachting werd aangericht onder de Tutsi-minderheid. De toenmalige FC van de VN-operatie in Ruanda (UNAMIR), generaal Romeo Dallaire, had New York van tevoren geïnformeerd over het feit dat hij beschikte over inlichtingen dat er een massale slachting stond te gebeuren. Hij vroeg toestemming om preventief te mogen optreden. UNAMIR beschikte over vrij nauwkeurige informatie waar zich geheime wapenopslagplaatsen bevonden en wilde deze

wapens in beslag nemen. New York zag het verhaal van Dallaire als het zoveelste paniekverhaal en misschien zelfs wel een poging tot manipulatie van de VN en weigerde toestemming. De slachting die volgde was van Bijbelse proporties waarbij UNAMIR machteloos moest toezien. Dit incident vond weliswaar plaats voordat ik in New York aantrad, maar ik heb er vele malen over gesproken met generaal Dallaire, die er tot op de dag van vandaag over tobt. Het is illustratief voor het wantrouwen van de VN ten opzichte van het product inlichtingen en de angst van de organisatie om gemanipuleerd te worden. In dit geval waren de inlichtingen echter correct.

### **Informele structuren**

Eigenlijk heb ik in het voorgaande deel al iets aangegeven over het feit dat er binnen het Secretariaat, naast de formele structuur op dit gebied, ook een informele structuur is gegroeid. Het op persoonlijke basis verstrekken van inlichtingen aan diverse VN-functionarissen in DPKO en DPA, heeft ertoe geleid dat er veel informele informatienetwerken bestaan. De informatie is vaak echter moeilijk te verifiëren en het is derhalve gevaarlijk om er ingrijpende beslissingen op te baseren. Soms is het mogelijk om verificatie te verkrijgen door informatie, afkomstig uit meerder informele netwerken, te vergelijken. Dit is echter geen eenvoudig proces. Een andere methode die kan worden gebruikt, is om de humanitaire organisaties binnen het VN-systeem te gebruiken om bepaalde informatie te controleren op juistheid. Immers, in potentie heeft het VN-systeem een enorme capaciteit om informatie te verzamelen en derhalve inlichtingen te produceren; organisaties zoals UNDP, UNHCR, WFP, UNICEF etc., zitten letterlijk overal ter wereld.

Indien deze ruwe informatie op de juiste manier geanalyseerd zou kunnen worden door mensen die hiervoor zijn opgeleid, kan dit leiden tot een goed inlichtingenproduct. Het probleem is echter dat het humanitaire

deel van de VN er niets voor voelt om op deze wijze door hun broeders in het politiek-militaire deel van het VN-systeem gebruikt te worden. Niet alleen omdat dit strijdig is met de ethiek van deze organisaties, maar ook omdat dit kan leiden tot enorme fysieke risico's voor hun personeel bij de uitvoering van hun humanitaire taak.

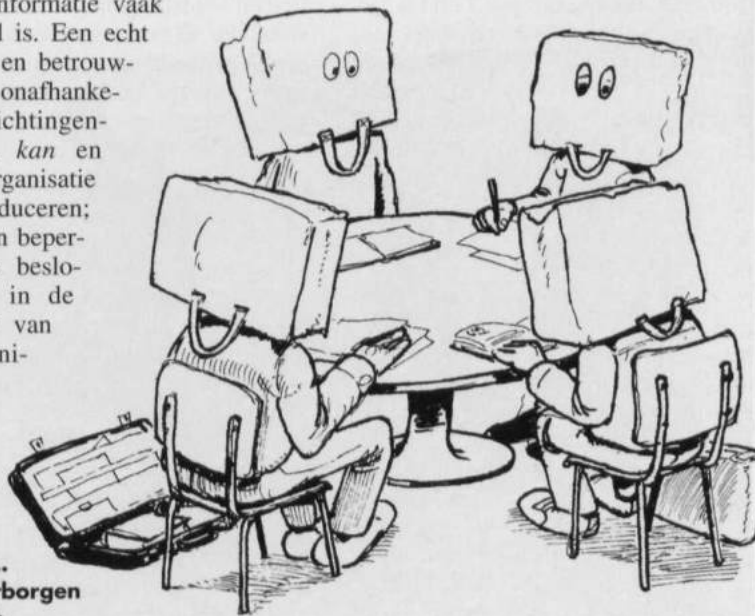
### **Slotopmerkingen**

Ik eindig deze bijdrage niet met conclusies en aanbevelingen, omdat ik daartoe nauwelijks in staat ben. Ik laat dit graag over aan anderen die meer ervaring hebben op inlichtingengebied. Ik heb slechts getracht om een deel van mijn ervaringen op dit gebied, gedurende mijn periode als militair adviseur van de SGVN, te beschrijven. Uiteraard is deze beschrijving niet neutraal, omdat de ervaringen daarvoor te persoonlijk zijn en derhalve gekleurd door mijn eigen opvattingen en interpretaties.

Als ik me dan toch wil wagen aan iets dat op een aanbeveling lijkt, dan denk ik dat het verstandig is voor een land als Nederland om zich te realiseren dat de VN weliswaar beschikt over heel veel informatie, maar dat de informatie vaak niet hard is. Een echt degelijk en betrouwbaar en onafhankelijk inlichtingenproduct, kan en wil de organisatie niet produceren; het is een beperking die besloten ligt in de structuur van de organisatie.

Een ander aspect dat ik wil benadrukken, is dat conflictbeheersing in internationaal verband op zijn minst gezegd niet politiek neutraal is. Er staan vaak grote belangen op het spel, zowel politiek, militair als anderszins en dat impliceert dat er door belanghebbenden inlichtingenactiviteiten worden ontplooid over het gehele spectrum. Actieve deelname aan crisisbeheersingsoperaties houdt onvermijdelijk in dat men met deze activiteiten wordt geconfronteerd. Het blind opereren in een dergelijke situatie brengt grote risico's met zich mee. Het lijkt mij dan ook verstandig om in ieder geval nationaal te kunnen beschikken over een eigen hoogwaardige capaciteit, om de veelheid aan beschikbare informatie te kunnen analyseren en zo tot een eigen oordeel te komen over de risico's en de wenselijkheid actief betrokken te worden bij de uitvoering van dit soort operaties.

Kort en goed, ik denk persoonlijk dat indien Nederland wil participeren in *Peace Support of Crisis Response Operations*, het van belang is om te kunnen beschikken over een goede inlichtingenorganisatie.



**Open overleg... geen verborgen agenda's**

# Intelligence en vredesoperaties

drs. R. Theunens\*

## De gewijzigde geostrategische omgeving<sup>1</sup>

Tot het begin van de jaren negentig waren de militaire inzetdoctrines en -concepten toegespitst op operaties van collectieve verdediging, ook wel 'Artikel V Operaties' genoemd. Dit gold ook voor de inlichtingendoctrine.

Tijdens het afgelopen decennium is hierin geleidelijk verandering gekomen en zijn de zogenaamde vredes- (ondersteunende) operaties op de voorgrond getreden. Vredes- (ondersteunende) operaties passen in het kader van conflictpreventie en crisisbeheersing (crisismanagement) en

worden uitgevoerd onder het Hoofdstuk VI, VII of VIII van het VN-Charter. In de vakliteratuur heeft men het over *peacemaking*, *peace-enforcement*, *peace-implementation*, *peace-building* en *peacekeeping*.

Recente ervaringen tijdens met name de UNPROFOR, UNOSOM en UNAMIR-operaties<sup>2</sup> hebben aangetoond dat een vredesoperatie, welke ook haar mandaat weze, inderdaad een adequate inlichtingenondersteuning vergt en bij voorkeur over een volwaardige, eigen inlichtingencapaciteit dient te beschikken. De afwezigheid van een dergelijke ondersteuning of capaciteit kan ernstige gevolgen hebben, niet

alleen voor de uitvoering van de opdracht, maar ook voor de veiligheid van de eigen troepen.

Anderzijds hebben begrippen zoals *Revolution in Military Affairs* (RMA),<sup>3</sup> *Low Intensity Conflict* (LIC),<sup>4</sup> *Asym-*



Inlichtingen zijn ook tijdens vredesoperaties noodzakelijk (Bron: foto Hennie Keeris)

\* De auteur was van 1992 tot 2000 Balkan-inlichtingenanalist bij SGR (Belgische militaire inlichtingen- en veiligheidsdienst) en tussen 1994 en 1999 verscheidene malen in inlichtingenfuncties in de hoofdkwartieren van UNPROFOR/UNPF, UNTAES en SFOR werkzaam. Sinds juli 2001 werkt hij als inlichtingenanalist bij het ICTY. Dit artikel is op persoonlijke titel geschreven en de opvattingen van de auteur reflecteren niet noodzakelijk die van SGR, de VN en/of het ICTY.

<sup>1</sup> Voor meer achtergrondinformatie over dit thema: Global Trends 2015: A Dialogue About the Future with Nongovernment Experts - Report by the National Intelligence Council. CIA (2000).

<sup>2</sup> Zie met name: Report of the Secretary-General Pursuant to General Assembly Resolution 53/35 (1998) Srebrenica Report (paragrafen 237, 474, 486 en 487); Verslag van de Parlementaire Commissie inzake Rwanda, Brussel (1997); Report of the Somalia Commission of Inquiry, Ottawa (1997).

<sup>3</sup> Revolution in Military Affairs: ook wel 'virtuele' oorlog genoemd. RMA leunt nauw aan bij de huidige conventionele conflicten, zij het dat dit soort conflicten worden gekenmerkt door de inzet van hoog technologische wapens tegen de 'centres of gravity' van de vijand (Command and Control, kritische infrastructuur enzovoort), voordat de confrontatie met de eigenlijke strijdkrachten wordt aangegaan.

<sup>4</sup> Low Intensity Conflict: guerrilla en terrorisme toegepast door revolutionaire en/of nationalistische groepen met doorgaans een beperkt aantal slachtoffers en beperkte schade voor gevolg. Gelet op het lange aanslepen van dergelijke conflicten, kan het aantal slachtoffers toch grote proporties aannemen. Er is bij dit soort conflicten vaak geen duidelijke frontlijn.

*metric Warfare*<sup>5</sup> enzovoort, hun intrede gedaan. Zonder in details te willen treden, kan worden gesteld dat LIC en asymmetrische operaties (ook) een zeer specifieke inlichtingenondersteuning vragen, met weliswaar niet noodzakelijk dezelfde invulling, maar wel een gelijkaardige, ingrijpende impact op de 'traditionele' inlichtingenorganisatie en -doctrine,<sup>6</sup> als het geval is bij vredesoperaties.

Of het nu om vredesoperaties, LIC of asymmetrische oorlogsvoering gaat, al deze operaties hebben gemeen dat er, zeker voor wat betreft het kader waarbinnen de inlichtingen- en veiligheidsdiensten opereren, geen onderscheid meer kan worden gemaakt tussen oorlog en vrede. In de praktijk is het zo dat het voor de veiligheids- en inlichtingendiensten eigenlijk altijd 'oorlog' is. Hun structuur moet voldoende sterk (met name inzake het personeelsaantal) en flexibel zijn om deze uitdaging succesvol aan te kunnen gaan. Bovendien hebben de inlichtingendiensten meer dan ooit een alarmbelfunctie, ook wel *indication and warning* (i&w) genoemd. De professionele uitbouw van een *indication and warning*-functie is een noodzakelijke voorwaarde om de evolutie en escalatieniveaus van de relevant geachte politieke, militaire, economische, culturele en andere parameters inzake de dreiging te kunnen meten, volgen en evalueren.

Een andere factor die in dit kader het vermelden waard is, is de sterk toegenomen invloed van de (internationale) media. Ze zijn van louter *opinion shapers* getransformeerd in prominente *policydrivers*, die naar gelang de situatie, een niet te onderschatten invloed op de politieke besluitvorming hebben. Zoals we verder zullen zien, is er in het bijzonder in vredesoperaties, een sterke wisselwerking tussen de media enerzijds, en het inlichtingenwerk anderzijds.

Dit artikel tracht een overzicht te geven van de specifieke eisen die vredesondersteuningsoperaties aan het inlichtingenwerk stellen. Het tracht ook voorstellen te formuleren voor

een adequatere inlichtingenorganisatie en -doctrine.

### Andere dreiging - andere opdracht

De dreiging in een vredesondersteunende operatie (of bij asymmetrische oorlogsvoering) is over het algemeen diffuser en moeilijker te identificeren. Daar waar we in ('traditionele') collectieve verdedigingsoperaties worden geconfronteerd met een kwantitatief en kwalitatief goed omlijnde en relatief eenvoudig in te schatten dreiging, die in de eerste plaats van militaire aard is en qua localisatie en geografische kenmerken gekend is, is dit bij asymmetrische oorlogsvoering in het algemeen en bij vredesondersteunende operaties in het bijzonder, meestal niet het geval.

Geregelde strijdkrachten spelen een ondergeschikte rol, terwijl (on)gecontroleerde paramilitaire 'vrijwilligers'-groepen of andere moeilijk te onderscheiden conflicterende elementen (inclusief criminele groeperingen en de burgerbevolking) het initiatief hebben. Bovendien zijn veel moeilijker te kwantificeren en kwalificeren politieke of socioculturele factoren determinerend voor de doelstellingen en de houding van de antagonist. Terwijl in 'traditionele' operaties de inlichtingenbehoefte zich in de eerste plaats in het militaire domein situeert, betekent dit dat in een vredesoperatie (en ook bij LIC en asymmetrische oorlogsvoering) er vraag is naar politieke, culturele, geografische, etnische, linguïstische, sociale, sociologische, historische, biografische, economische, demografische, religieuze, ecologische enz. inlichtingen. De kennis en het begrip van al deze facetten is een noodzakelijke voorwaarde om de motieven en de aspiraties van de conflicterende partijen te kunnen onderkennen en dus een adequate inlichtingenondersteuning te kunnen leveren. Bovendien zullen niet alleen het potentiële geografische inzetgebied, maar ook het *area of intelligence interest* (AOI) veel groter zijn bij vredesoperaties.<sup>7</sup>

Dit alles kan als volgt worden samengevat: het omgevingskader van militaire operaties is bij vredesoperaties geëvolueerd van een *military information environment* naar een *global information environment*.

Het veel ruimere en gediversifieerde inlichtingenstudiegebied enerzijds, en de verwerking van de veel grotere hoeveelheid aan informatie anderzijds, stellen bijzondere eisen aan de capaciteiten en opleiding van het inlichtingenpersoneel. Zo heeft bijvoorbeeld in het analysedomein, linkanalyse, ondersteund door gespecialiseerde software, aanzienlijk aan invloed gewonnen.

Belangrijk is ook in te zien dat, aangezien het de basis vormt voor het (politieke) besluitvormingsproces inzake de deelname aan de vredesoperatie, het hierboven beschreven multidisciplinaire inlichtingenbeeld, reeds vóór het eigenlijke uitsturen van de vredestroepen beschikbaar moet zijn. Analooft verdient het aanbeveling dat een deel van het inlichtingenpersoneel wordt ontplooid voor de aankomst van het gros van de vredesmachtroepen.

Het is in dit licht interessant even stil te staan bij de lessen die getrokken zijn uit de Kosovocrisis van het voorjaar 1999. Het *Defence Committee of the UK House of Commons*<sup>8</sup> schrijft onder andere dat:

*"het een vergissing is te denken dat inlichtingen in de eerste plaats tot doel hebben de toekomst en de*

<sup>5</sup> Voor meer achtergrondinformatie over dit thema: Kevin 'O'Brien en Joseph Nusbaum - Intelligence Collection for Asymmetric Threats, part one and part two. *Jane's Intelligence Review*, oktober en november (2000).

<sup>6</sup> David Charters - 'Virtual War? Virtual intelligence?' Alternative Visions of Future War and Intelligence. Lezing op CASIS conference, Ottawa (september 2000).

<sup>7</sup> Andrei Raevsky - Managing Arms in Peace Processes: Aspects of Psychological Operations and Intelligence. UNIDIR, Genève (1996).

<sup>8</sup> Lessons of Kosovo, Volume I, Reports and Proceedings of the Committee, Defence Committee, Fourteenth Report, House of Commons, Londen, 23 oktober 2000.

acties van de tegenstrever met grote zekerheid te voorspellen. De echte finaliteit van inlichtingen bestaat erin de mogelijke opties en reacties van de tegenstrever te onderscheiden en te analyseren, zelfs als die irrationeel zouden lijken, zodanig dat de planners en beleidsverantwoordelijken er rekening mee kunnen houden en niet het risico lopen door de gebeurtenissen te worden verrast. Anderzijds moeten de beleidsverantwoordelijken hun inlichtingenbehoefte duidelijk bepalen en de inlichtingen die ze krijgen, kritisch beoordelen. De inlichtingendiensten dienen in ruimere mate het advies van de buitenwereld (academici, NGO's enzovoort) in te winnen."

Deze lessen kunnen, wanneer we ze vergelijken met de traditionele aanpak, als enigszins revolutionair worden bestempeld.

Een ander belangrijk verschil tussen collectieve verdedigingsoperaties en vredesoperaties situeert zich in de operationele doelstellingen en prioriteiten. Bij een operatie van collectieve verdediging bestaat de opdracht erin het grondgebied van de alliantie te verdedigen tegen een agressie door derden (en indien mogelijk deze laatste verslaan). In een vredesondersteunende operatie kan de opdracht bestaan uit conflictpreventie, scheiding van de strijdende partijen, bemiddeling, humanitaire hulpverlening, evacuatie van ingezetenen enzovoort.

In de praktijk blijkt dat in vredesondersteunende operaties, *force protection* de beperkende factor is op de uitvoering van deze opdracht. *Force protection* impliceert dat er bijzondere aandacht aan het aspect contra-inlichtingen (subversie, spionage en terrorisme) wordt besteed. *Force protection* is ook het domein bij uitstek om de invloed van de media te illustreren. De evolutie van de maatschappelijk aanvaardbare normen inzake verliezen, waarbij in de hedendaagse westerse samenleving, enkele uitzonderingen nagelaten, nog slechts *zero*

losses acceptabel zijn voor de publieke opinie, hebben de invloed van de media aanzienlijk versterkt. Terwijl de media via *open source intelligence* (OSINT) een belangrijke bron van inlichtingen zijn, kan hun invloed, ten gevolge van de niet noodzakelijk steeds waarheidsgetrouwe percepties die ze durven propageren, contraproductief werken.<sup>9</sup> De inlichtingendiensten komen in een soort van concurrentiepositie terecht, waarbij ze al voor de aanvang de strijd hebben verloren, omdat ze niet kunnen optornen tegen de snelheid waarmee massamedia blikvangers, van om het even waar, in de wereld kunnen brengen. Toch wordt van de inlichtingendiensten verwacht, dat ze de mediaberichtgeving binnen minimale termijnen aan een kritisch onderzoek kunnen onderwerpen en alle door de media opgeworpen vragen kunnen beantwoorden.

### Impact op de inlichtingenorganisatie

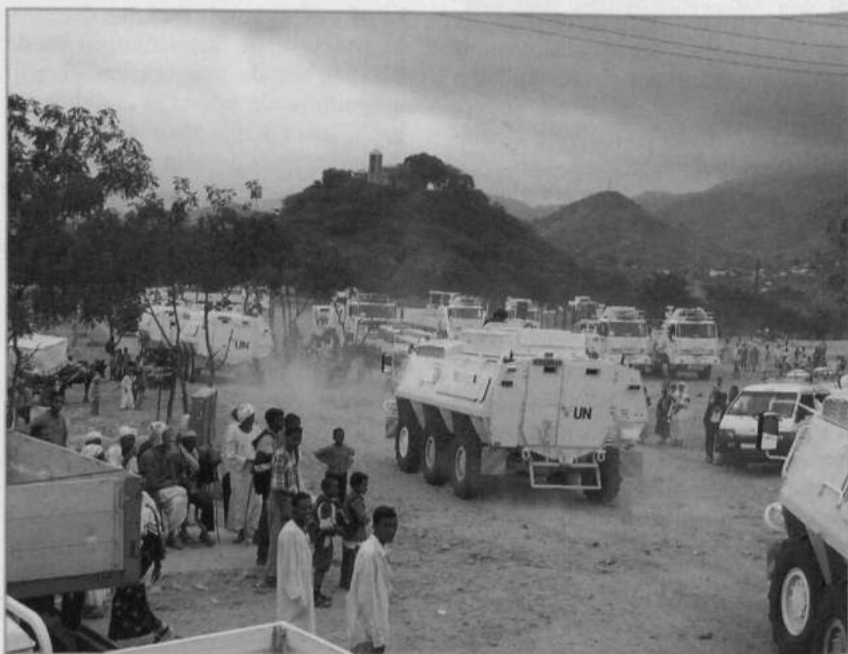
Het hierboven beschreven onderscheid heeft een diepgaande weerslag

op de aard van de vereiste inlichtingen en dus ook op de inlichtingendoc-trine, -organisatie en procedures.

### 'Intelligence' versus 'military information'

Het handhaven van de neutraliteit en transparantie zijn twee basisprincipes van vredesondersteunende operaties. De vredesmacht kan haar opdracht slechts uitvoeren als ze het vertrouwen geniet van de betrokken partijen; in het bijzonder van de lokale bevolking. Een te actieve inlichtingenopsporingsinspanning kan als agressief, niet geoorloofd of zelfs als 'spionage' (en dus een vijandelijke daad) worden geïnterpreteerd, niet alleen door de strijdende partijen, maar ook door andere landen die troepen leveren voor de operatie. Op die manier wordt de geloofwaardigheid van en het (interne) vertrouwen in de vredesmacht gehypothekeerd. Gezien de mogelijk negatieve connotatie van het begrip 'inlichtingen' heeft de VN het over 'militaire informatie'.<sup>10</sup> Het stre-

<sup>9</sup> Zie rol CNN-factor en het zogenaamde IRMA-effect (Instant Response to Media Attention).



Handhaving neutraliteit en transparantie: twee basisprincipes van vredesondersteunende operaties (Bron: foto Hennie Keeris)

ven naar transparantie uitte zich tijdens de UNPROFOR-operatie met name door het gebruik van niet-vercijferde communicatiemiddelen van het type *Motorola* om de verbindingen tussen het hoofdkwartier en de eenheden te velde te verzorgen, met alle gevolgen van dien voor de veiligheid van de operaties.<sup>11</sup>

#### Onderscheid tussen tactische, operationele en strategische inlichtingen

In tegenstelling tot een operatie van collectieve verdediging, is bij een vredesoperatie het onderscheid tussen tactische, operationele en strategische ontwikkelingen (en dus inlichtingen) doorgaans onduidelijk. Tactische ontwikkelingen (bijvoorbeeld een schietpartij met lichte wapens) kunnen strategische implicaties hebben (als er slachtoffers vallen in de rangen van de vredesmacht) en vice versa. Het structureel scheiden van deze quasi gelijkaardige en elkaar wederzijds beïnvloedende niveaus, zoals het geval is in de inlichtingenorganisatie van traditionele krijgsmachten, is hoogst contraproductief in vredesoperaties. De inlichtingenstructuur (en dus ook haar personeel) moet flexibel zijn om de permanente integratie en synthese van de drie disciplines (tactisch, operationeel en strategisch) toe te laten.

#### Andere klemtoon:

##### intenties versus capaciteiten

In een 'traditionele' collectieve verdedigingsoperaties ligt de klemtoon op de studie van de (meetbare) militaire capaciteiten (*capabilities*) van de tegenstrever (wat kan hij? waar?). Bij vredesoperaties en asymmetrische oorlogsvoering is de kennis van de capaciteiten van de partijen ondergeschikt aan het inzicht in hun intenties (*intent*: wat willen ze?) en motieven (waarom?), zonder hierbij echter de capaciteiten uit het oog te verliezen. De intenties en motieven zijn zoals eerder beschreven veel ruimer dan de louter militaire capaciteiten. Ze kunnen in sommige gevallen naar onze logica irrationeel lijken. Sensoren en detectoren die in een traditioneel conflict volstaan om een

goed beeld van de vijandelijke capaciteiten en mogelijkheden te vormen (ISTAR), zullen in crisispreventie- of -beheersingsomgeving slechts een betrekkelijke waarde hebben. Het 'begrijpen' van de partijen kan niet aan sensoren of detectoren worden overgelaten, maar is een louter menselijke taak, die specialisatie en flexibiliteit – twee niet noodzakelijk verenigbare kwaliteiten – van het inlichtingenpersoneel vraagt.

#### Andere disciplines: HUMINT en OSINT versus SIGINT en IMINT – weerslag invloed op de analysecapaciteit

Het belang van *intent* versus *capability* heeft voor de inlichtingenorganisaties tot gevolg dat, terwijl in een collectieve verdedigingsoperaties, SIGINT (COMINT en ELINT), *Imagery Intelligence* (IMINT) en *Measurement and Signature Intelligence* (MASINT) de dominerende disciplines zijn, in een vredesoperatie OSINT en vooral HUMINT primeren.<sup>12</sup> OSINT impliceert ook de uitbating van lokale media. Dit betekent concreet niet alleen de inzet van personeel dat de lokale taal begrijpt of tolken, maar ook het risico van misleiding door propaganda.

De overheersende waarde van HUMINT brengt met zich mee, dat ook andere militairen dan de traditionele collectors<sup>13</sup>, informatie kunnen opsporen en verwerven. Logistieke en humanitaire konvoeien verplaatsen zich door de volledige actiezone heen en zijn dus zeer waardevolle potentiële collectors. Hetzelfde geldt voor genie, bindings- en medisch personeel, en CIMIC- en PsyOps-teams. Liaisonofficieren onderhouden bevoorrechte contacten met de lokale autoriteiten en zijn dus, indien goed aangewend, potentieel bronnen die van onschatbare waarde kunnen zijn. Dit betekent dat al het personeel van het belang van inlichtingen dient te worden doordrongen en dus een basisvorming in dit domein moet krijgen. De toename van het aantal, vaak onervaren, collectors (die allen moeten worden gedebriefd) vergroot het risico op *information overload* en, erger nog, op desinformatie. Er dienen

dan ook filters te worden voorzien, zoals bijvoorbeeld een analysecapaciteit op het echelon van de S2-bataljon, analyseondersteunende software en databanken enzovoort. Het spreekt voor zich dat de toename van het aantal opsporingsinstrumenten en hun diversiteit, een goed functionerende *Collection Coordination Requirements Management* (CCIRM) vragen.

Een niet te verwaarlozen factor in dit verband is dat de internationale organisatie die de vredesondersteunende operatie leidt, *rules of engagement* (ROE's) kan opleggen die de inzet van bepaalde opzoekingsinstrumenten (SIGINT, *covert* HUMINT enzovoort) verbiedt of beperkt.<sup>14</sup> Het is duidelijk dat dit de opsporingscapaciteit kan aantasten en er naar alternatieven moet worden gezocht (bijvoorbeeld via nationale inlichtingenkanalen).

Te agressieve HUMINT (die als spionage zou kunnen overkomen) kan in een vredesondersteunende operatie het wantrouwen van de partijen uitlokken en op die manier de operatie in diskrediet brengen. De operatoren die

<sup>10</sup> Daniel Villeneuve – Intelligence and the United Nations, Lessons from Bosnia. *Military Intelligence*, oktober-december (1996).

<sup>11</sup> Het volstond voor de strijdende partijen om deze communicatiemiddelen buit te maken om toegang tot de communicaties te hebben. De landen die troepen bijdroegen pasten kunstgrepen toe zoals het gebruik van nationale vercijferbare communicatiemiddelen, of meer rudimentair, het gebruik van dialect in de communicaties.

<sup>12</sup> Dit betekent echter niet dat SIGINT en IMINT geen bijdrage kunnen leveren. UAV's (Unmanned Aerial Vehicle) zijn zeer nuttig om verkenningen uit te voeren van moeilijk toegankelijke gebieden en derhalve bijzonder geschikt voor de controle van de demilitarisatie van bepaalde zones, en de verificatie van de naleving van separatie- of bufferzones. Observatiesatellieten zijn essentieel voor I&W (early warning).

<sup>13</sup> (Gespecialiseerde) verkenningseenheden, eenheden in lijn, HUMINT-operatoren, et cetera.

<sup>14</sup> Zoals bijvoorbeeld SIGINT en actieve HUMINT in het geval van UNPROFOR. Sommige troepenleverende landen ondernamen echter de nodige demarches om via nationale weg hieraan te remediëren (met name de UK met de Joint Commission Observers (JCO)).

nen dus discreet en fijngevoelig te werk te gaan, en de plaatselijke gebruiken en gevoeligheden (alsook de lokale taal) te kennen. Coördinatie met CIMIC- en PsyOps-teams is belangrijk. (Duurzame) HUMINT veronderstelt bovendien een bijzondere inspanning inzake bronbescherming.

De grote handicap voor HUMINT in vredesondersteunende operaties is, dat ten gevolge de tijdsdruk en de rotaties van het personeel van de vredesmacht, contacten en bronnen vaak onvoldoende kunnen worden 'gescreend'. Er is dus een risico op infiltratie en misleiding (desinformatie) door ongewenste elementen. De motieven van de contacten en bronnen om met de vredesmacht samen te werken, zijn niet altijd even nobel. Dit kan een negatieve invloed hebben op de kwaliteit van de door hen geleverde informatie.

De massale input aan HUMINT en OSINT brengt met zich mee, dat het belang van een performante menselijke analysecapaciteit bij een vredesondersteunende operatie veel groter is dan bij een collectieve verdedigingsoperatie. Daarbij komt dat die analysecapaciteit over een gedegen kennis van de historische, culturele, sociale, demografische en sociologische aspecten van het conflict moet beschikken. In plaats van louter de militaire aspecten van de 'vijand' te analyseren, moeten nu *alle* partijen, aanwezig in het *area of interest*, worden bestudeerd, en dit in *alle* facetten. Er is dus een noodzaak aan geschoold personeel met een expertise die het militaire kader overstijgt. Hieraan kan worden tegemoet gekomen door werving van burgeranalisten met een relevante studieachtergrond of andere ervaring.

#### Fusion - Liaison - Releasability

De (militaire) vredesmacht opereert in een vredesondersteunende operatie niet autonoom, maar in het kader van een door een (internationale) civiele autoriteit geleide operatie.<sup>15</sup> Deze realiteit heeft belangrijke implicaties voor het inlichtingendomein. Teneinde de inlichtingenopdracht (in het bijzonder *force protection*) tot een goed



Een wereld vol geweld (Bron: foto Martin Roemers)

einde te kunnen brengen, is het voor de militaire inlichtingenorganisatie vitaal een coherent beeld te hebben van de politieke, sociale, sociologische, economische en culturele toestand en hun mogelijke evolutie. Meestal beschikt de militaire inlichtingenorganisatie echter niet over al deze informatie en moet ze een beroep doen op de civiele organisaties (*UN Civil Affairs*, EU of OVSE-waarnemers, NGO's) die in de zone actief zijn.<sup>16</sup> Omgekeerd hebben de burgerorganisaties (in het bijzonder politieke en humanitaire organisaties) militaire inlichtingen (bedreigingsanalyses, humanitaire informatie enzovoort) nodig. Er moeten dus procedures en structuren bestaan voor het samenbrengen en uitwisselen van deze informatie en inlichtingen. Dit laatste stelt, naast een begrip van elkaars bedrijfscultuur, bijzondere eisen inzake liaison en *releasability*. Gelet op de afwijkende bedrijfscultuur, is met name een sensibilisatie van de burgerlijke organisaties voor begrippen als bronbescherming en *need to know* aangewezen.

*Releasability* kan ook een probleem vormen bij ad hoc-allianties zoals SFOR en KFOR, waarbij sommige partners geen deel uitmaken van de bestaande bondgenootschappen. Die coalitiepartners kunnen de indruk krijgen dat de alliantie hen de toegang tot vitale inlichtingen ontzegt ('ze achterhoudt'), of erger nog, inlichtingen over hen wil verzamelen.<sup>17</sup>

Een politiek zeer gevoelig (en controversieel) aspect in dit domein is de vrijgave van inlichtingen, die via

<sup>15</sup> Vergelijk UNPROFOR/UNPF en UNTAES enerzijds en SFOR, KFOR anderzijds. Bij UNPROFOR/UNPF en UNTAES was de civiele autoriteit (Special Representative of the Secretary General, of, wat UNTAES betreft, de Transitional Administrator) de algehele chef van de vredesoperatie. In BiH bestaat geen subordinaatiebetrekking tussen OHR en UNMIBH enerzijds en COMSOF anderzijds. Dit is evenmin het geval in Kosovo tussen de SRSG UNMIK en COMKFOR.

<sup>16</sup> Pär Erikson - Civil-Military Coordination in Peace Support Operations - An Impossible Necessity, *The Journal Of Humanitarian Assistance*, Stockholm, 1999.

nationale kanalen beschikbaar zijn, aan de vredesmacht. Zeker voor kleinere landen als Nederland en België, kan het vrijgeven van via eigen kanalen verkregen inlichtingen aan de vredesmacht te velde, of aan de internationale organisatie die de operatie leidt, vruchten afwerpen. Het leveren van een specifieke inlichtingenondersteuning kan er namelijk voor zorgen, dat de internationale besluitvorming meer rekening houdt met de soms specifieke inzetomstandigheden van onze troepen,<sup>18</sup> en, in navolging van het *quid pro quo*-principe, inlichtingen ontsluiten waartoe we anders nooit toegang zouden hebben.

Uit dit alles blijkt dat er procedures voor (de)classificatie en vrijgeven van informatie en inlichtingen dienen te worden vastgelegd vóór het begin van de operatie.

De ervaringen met UNPROFOR, en vervolgens met het CJTF-concept (IFOR, SFOR en KFOR) in de Balkan, tonen aan dat de problemen voor het vrijgeven en delen van informatie en inlichtingen pertinent zijn. In 1995 was het hoofd van de *Military Information*

*Branch* van het hoofdkwartier UNPROFOR/UNPF afkomstig uit een niet-NAVO-land. Zijn Amerikaanse plaatsvervanger beschikte systematisch over informatie, soms van 'dubieuze' oorsprong,<sup>19</sup> die hij niet met zijn chef mocht delen, maar wel met landgenoten of sommige bevoorrechte partners (de *canukus*) binnen de staf. Deze toestand zorgde voor wrevel, niet in het minst bij personeel afkomstig uit niet bevoorrechte NAVO-landen uit de cel, die soms het gevoel hadden 'buitenspel te worden gezet'.

Bij de ontplooiing van IFOR, na de ondertekening van het vredesakkoord van Dayton, in december 1995, stond aanvankelijk de scheiding van de voormalige strijdende partijen, om het heropflakkeren van de strijd te verhinderen, centraal. De inlichtingeninspanning was dan ook geconcentreerd op militaire en politieke inlichtingen. Na verloop van tijd trad de strijd tegen de corruptie (rol van georganiseerde misdaad en haar relaties met de politieke machthebbers) op de voorgrond en verschoof de prioriteit van de inlichtingeninspanning naar

criminele en economische inlichtingen. Inlichtingen over de demografische toestand (etnische verdeling van de bevolking, terugkeer van vluchtelingen) bleven tijdens de gehele implementatiefase belangrijk. Om deze informatie en inlichtingen te verwerven, moest SFOR een beroep doen op de civiele organisaties die in het gebied actief waren (zoals OHR, UNMIBH, EUMM en de OVSE) en moesten procedures en mechanismen voor de uitwisseling van de verschillende typen inlichtingen worden uitgewerkt. Nog tot zeker in het voorjaar van 1999 waren er geen duidelijke procedures voor de uitwisseling van gevoelige informatie tussen SFOR, UNMIBH en andere belanghebbenden.

## Conclusie

Vredesoperaties vergen een specifieke inlichtingenondersteuning die vaak ingrijpend afwijkt van traditionele collectieve verdedigingsoperaties. Aangezien de gewijzigde geostrategische omgeving en de evolutie van de dreiging op hun beurt ook een eigen inlichtingenondersteuning vragen, lijkt de tijd rijp om de traditionele inlichtingenorganisatie en -structuur door te lichten en aan te passen aan deze nieuwe uitdagingen.



Het gaat altijd om mensen (Bron: foto Martin Roemers)

<sup>17</sup> Andrei Raevsky - *Managing Arms in Peace Processes: Aspects of Psychological Operations and Intelligence*. UNIDIR, Genève, 1996. Dit was met name het geval in de UNCRO, UNTAES missie, waar sommige Russische stafofficieren ervan overtuigd waren dat NAVO-militairen (BE, NL, VS) die deel uitmaakten van de VN-operatie, hen 'bespioneerden'.

<sup>18</sup> Zie de Belgisch-Luxemburgse Battle Group BELUKOS, die zich in het noorden van Kosovo, in louter door Serviërs bewoond gebied bevindt. Haar inzetomstandigheden wijken af van die waarmee de andere contingents elders in Kosovo worden geconfronteerd.

<sup>19</sup> Met name tijdens de Operatie Storm in augustus 1995 (Kroatisch offensief tegen Krajina) werd duidelijk dat er ook in het inlichtingendomein bijzonder relaties bestonden tussen het land van herkomst van de plaatsvervangende G2 en Kroatië.



# De NAVO en inlichtingen

J.R. Karssing – generaal-majoor der cavalerie b.d.\*

*'Tell me what you know.  
Tell me what you don't know.  
Tell me what it means.  
And never confuse the three.'*  
General Colin Powell

## Inleiding

In dit artikel geef ik inzicht in de doelstelling, de structuur en de werkwijze van de NAVO-inlichtingenorganisatie. Vervolgens worden de problemen die daarmee gepaard gaan aan de orde gesteld. Het artikel rond ik af met een beschouwing over veranderingen, aanpassingen en bevindingen.

De doelstelling voor het verzamelen van inlichtingen in vreedstijd, gedurende crises en conflicten is het ondersteunen van de planning en uitvoering van militaire operaties door tijdig de juiste inlichtingen te verschaffen. Het Militair Comité (MC) moet hierdoor in staat worden gesteld haar rol als adviesorgaan te vervullen. Tegelijkertijd vormen inlichtingen één van de fundamenten voor de aanwijzingen en richtlijnen van dit Comité aan de Strategische Commando's (SC's).

Deze commandanten en hun ondergeschikten hebben inlichtingen nodig om hun opdracht met succes te kunnen uitvoeren. Inlichtingen die zij verzamelen kunnen weer relevant zijn voor de adviezen en besluiten van het MC. De NAVO-inlichtingenorganisatie moet dit bewerkstelligen.

## De inlichtingenorganisatie

Het zal niet verbazen dat de NAVO-inlichtingenorganisatie wordt beïnvloed door de complexiteit van het bondgenootschap. De belangrijkste actoren vormen het eerder genoemde MC, de Internationale Militaire Staf (IMS), de SC's, de *NATO Intelligence Board* (NIB) en de lidstaten, inbegrepen hun inlichtingendiensten. Het Militair Comité (MC) zorgt op militair gebied voor consultaties en samenwerking met en tussen lidstaten. Het MC is verantwoording verschuldigd aan de Noord-Atlantische Raad (NAR) en het Defensie Plannings Comité (DPC). Het adviseert de secretaris-generaal, de NAR en het DPC over militaire aangelegenheden. Het geeft aanwijzingen en richtlijnen aan de strategische commando's: *Allied Command Europe* (ACE) gevestigd in Mons, België en *Allied Command Atlantic* (ACLANT), met hoofdkwartier in Norfolk, vs.

Het MC wordt ondersteund door de Internationale Militaire Staf (IMS). In deze staf is ook de *Assistent Chief of Staff Intelligence* (ACOS-Int) opgenomen. Hij geeft leiding aan het proces van het verzamelen, verwerken en

verspreiden van inlichtingen binnen de NAVO. Hij is verantwoordelijk voor het inlichtingendeel van het advies aan de SG, de NAR en het DPC. Met name gaat het daarbij om het adviseren over ontwikkelingen die de belangen van de NAVO kunnen raken. De inlichtingenorganisatie van de IMS, de *Intelligence Division* bestudeert en vergelijkt de inlichtingen vanuit de hoofdsteden van de lidstaten en vanuit de Strategische Commando's. Zij analyseert de informatie en brengt op basis daarvan adviezen uit.

## De lidstaten

De NAVO is geen supranationale organisatie met een eigen, robuuste inlichtingenstructuur. De NAVO-landen zijn de voornaamste inlichtingenbronnen waar de verdragsorganisatie over beschikt. Elk land heeft, naar gelang de grootte van de militaire organisatie, een eigen specifiek ingerichte inlichtingenorganisatie. Ieder land heeft ook zijn eigen inlichtingenbelangstelling met een nationale inkleuring. Noorwegen, als voorbeeld, heeft een zeer gespecialiseerde kennis met betrekking tot alle activiteiten die in de buurt van haar territoriale wateren plaatsvinden.

Ieder land heeft zijn methoden om inlichtingen te verzamelen en zal immer trachten de gebruikte bronnen te beschermen. Door deze taakverdeling is de NAVO voor het grootste deel afhankelijk van de hoeveelheid en de kwaliteit van de inlichtingen die de lidstaten ter beschikking stellen.

\* De auteur bedankt H. Emmens, commodore KLU, W. van Looij, luitenant-kolonel van de verbindingdienst en V.A.C. Remouchamps, luitenant-kolonel der luchtdoelartillerie, voor hun commentaar en bijdragen. De auteur was Assistent Chief of Staff Intelligence (ACOS-Int)-SHAPE. De genoemde officieren zijn bij de Intelligence Division werkzaam.

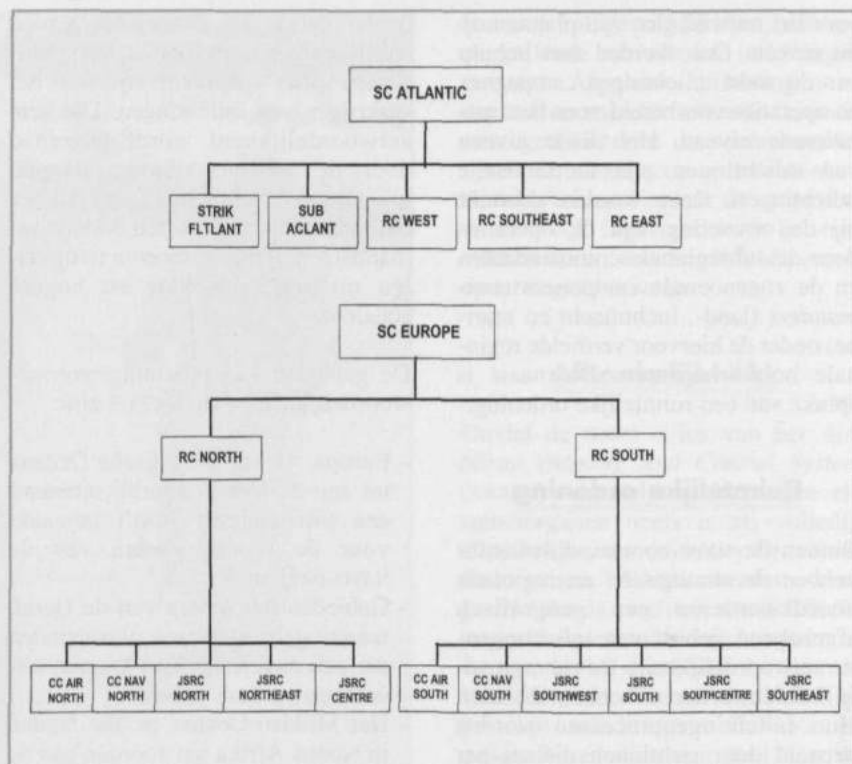
## De Strategische Commando's (sc's)

Zij geven invulling aan de aanwijzingen en de richtlijnen van de IMS en zijn ervoor verantwoordelijk dat deze richtlijnen worden uitgevoerd. Omdat deze richtlijnen moeten worden 'vertaald' voor de aan hen ondergeschikte regionale hoofdkwartieren moeten de sc's aanvullende inlichtingen hebben die geschikt zijn voor deze lagere niveaus. De sc's hebben behoefte aan alle noodzakelijke inlichtingen om in potentiële crisisgebieden opdrachten te kunnen uitvoeren. Wat SHAPE betreft kan een deel van deze aanvullende informatie afkomstig zijn van adviseurs van onder andere *National Security Agency* (VS), *Defence Intelligence Agency* (VS), *Defence Intelligence Service* (UK) en *Federal Armed Force Information Office* (GE), die in de staf van de inlichtingendivisie van dit commando zijn vertegenwoordigd.

## De NATO Intelligence Board (NIB)

De NIB is het hoogste discussieforum binnen de NAVO waarin gediscussieerd wordt over het inlichtingenbeleid. Ook worden afspraken gemaakt over problemen en verschillen van mening binnen de inlichtingenorganisaties van de diverse landen. Allerlei onderwerpen die met de productie van inlichtingen te maken hebben, worden hier besproken. Deelnemers aan dit forum zijn in principe de nationale hoofden van militaire inlichtingendiensten, vertegenwoordigers van de inlichtingenorganisatie van de IMS en de inlichtingenorganisaties van de sc's.

In het kort komt het erop neer dat de NAVO-landen de inlichtingen verstrekken; de IMS de verspreiding coördineert naar leden van de alliantie, het MC, de NAR en ten slotte naar de sc's, die de informatie gebruiken voor het ontwikkelen van hun plannen. Het is van het grootste belang dat alle beschikbare inlichtingen zo compleet



De NAVO-commandostructuur

mogelijk aan alle gebruikers ter beschikking worden gesteld. Indien informatie incompleet in het inlichtingenproces wordt binnengebracht, kan het uiteindelijke resultaat foutief zijn, hetgeen tot gevolg kan hebben dat een verkeerd advies wordt gegeven tijdens het besluitvormingsproces.

Hiermee wordt tevens een gevaarlijk facet van het systeem belicht. Politiek nationaal-gevoelige inlichtingen kunnen worden achtergehouden als ze geheel of gedeeltelijk passen in nationale scenario's. Met name de grotere NAVO-landen met een robuuste inlichtingenorganisatie hebben de neiging op bepaalde politiek gevoelige terreinen mondjesmaat inlichtingen aan de NAVO-inlichtingenorganisatie ter beschikking te stellen, en alleen als dit past in hun politieke perceptie van dat moment.

In het kader van het inlichtingenproces zijn twee begrippen relevant: inlichtingenniveaus en de geografie-

sche ordening in gebieden van inlichtingenverantwoordelijkheid en -belangstelling.

## Inlichtingenniveaus

Binnen het inlichtingengebied kunnen wij de drie niveaus onderscheiden: strategisch, operationeel en tactisch. Strategische inlichtingen worden gebruikt op het hoogste inlichtingenniveau. Zij zijn het resultaat van alle informatie die door de lidstaten ter beschikking zijn gesteld aan het NAVO-hoofdkwartier en/of de twee strategische hoofdkwartieren.<sup>1</sup> Deze inlichtingen bevatten internationale, diplomatieke, politieke, economische en militaire informatie. Het tweede niveau – het operationele – zijn de inlichtingen die door de regionale hoofdkwartieren worden gebruikt

<sup>1</sup> Tijdens deze bijdrage zal, indien dieper wordt ingegaan op 'Strategische Commando's', voornamelijk Allied Command Europe (ACE) worden behandeld.

voor het ontwikkelen van plannen op dit niveau. Ook worden met behulp van dit soort inlichtingen campagnes en operaties voorbereid voor het operationele niveau. Het derde niveau van inlichtingen zijn de tactische inlichtingen. Deze worden gebruikt bij de uitvoering van de operaties door de subregionale commandanten en de zogenoemde *component commanders* (land-, luchtmacht en marine) onder de hiervoor vermelde regionale hoofdkwartieren. Daarnaast is sprake van een ruimtelijke ordening.

### Ruimtelijke ordening

Binnen de NAVO-commandostructuur hebben de strategische en regionale hoofdkwartieren een geografisch afgebakend gebied van inlichtingenverantwoordelijkheid. De subregionale hoofdkwartieren hebben dit niet. Hun inlichtingenprocessen worden bepaald door richtlijnen die zij per opdracht van de regionale commandanten ontvangen.

Binnen het gebied wordt aangegeven welke commandanten verantwoordelijk zijn voor het verkrijgen van inlichtingen. Die verantwoordelijkheid wordt begrensd door de ter beschikking staande inlichtingenverzamelorganen. Bij het ontbreken daarvan, zullen ondercommandanten derhalve moeten terugvalen op nevensgeschikte en hogere echelons.

De gebieden van inlichtingenverantwoordelijkheid voor SACEUR zijn:

- Europa, van de Atlantische Oceaan tot aan de Oeral, waarbij uiteraard een uitzondering wordt gemaakt voor de grondgebieden van de NAVO-landen;
- Gebieden ten oosten van de Oeral, waarin gebeurtenissen plaatsvinden die een directe invloed kunnen uitoefenen op deze gebieden;
- Het Midden-Oosten en alle landen in Noord-Afrika ten noorden van de Kreeftskring alsmede alle terri-

toriale wateren in de Oost-Atlantische Oceaan, zeestraten en overige wateren die grenzen aan het de West-Europese grondgebieden.

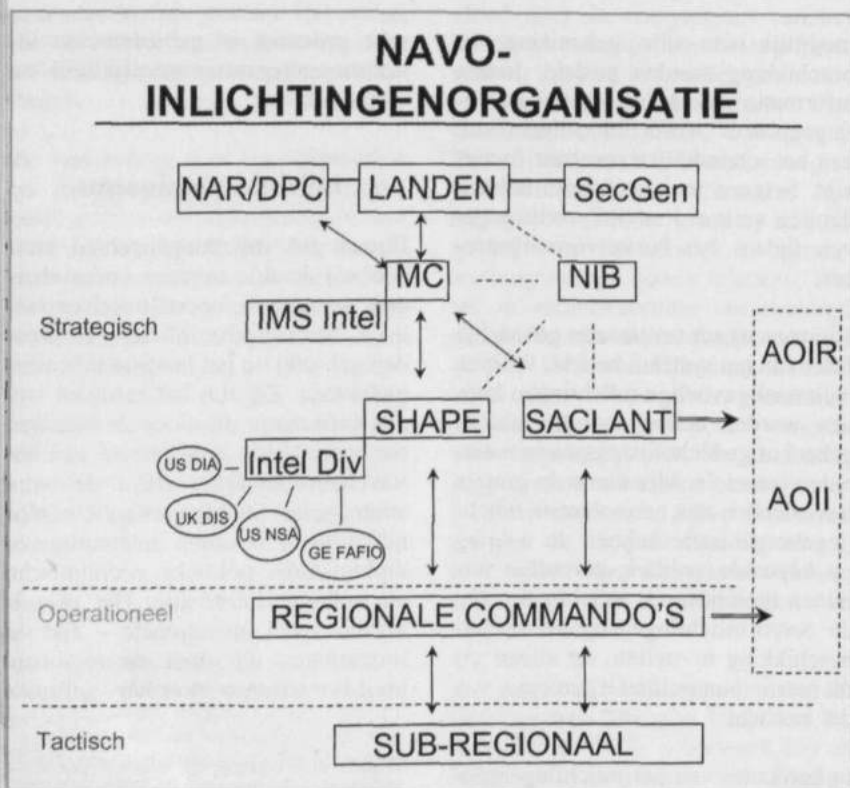
In het algemeen grenst het gebied van inlichtingenbelangstelling (*Area of Intelligence Interest* (AOII)) aan het geografisch gebied van inlichtingenverantwoordelijkheid.

Uitzonderingen zijn mogelijk. Als voorbeeld kunnen twee voor SACEUR belangrijke onderwerpen worden genoemd: terrorisme en proliferatie. Terrorisme is relevant als exponent van asymmetrische oorlogvoering. Met terreurdaden moet steeds rekening worden gehouden. Wat proliferatie betreft gaat de aandacht uit naar India, Pakistan en Noord-Korea.

De betrokken landen zijn niet geografisch aangrenzend. Daarom zal het noodzakelijk zijn om zijn inlichtingen uit andere bronnen te krijgen. Dit betekent voor SACEUR dat interesse bestaat in alle gebieden die een mogelijke invloed zouden kunnen uitoefenen op het uitvoeren van zijn opdracht in de meest ruime zin. Het betekent onder meer dat alle landen die een rol spelen op het gebied van wapenproductie en wapenexport zijn belangstelling hebben, in het bijzonder landen die een rol spelen op het gebied van de ontwikkeling en verspreiding van massavernietigingswapens, zoals de eerder genoemde drie, alsmede China.

### Het inlichtingenproces binnen de NAVO

Zoals binnen iedere militaire organisatie beginnen alle activiteiten die moeten leiden tot het uitvoeren van een opdracht met het geven van een opdracht. De interpretatie door de commandant van die opdracht leidt tot het vaststellen van de behoefte aan inlichtingen die hij nodig heeft om zijn opdracht met succes te kunnen uitvoeren. De voornaamste behoefte aan inlichtingen, - vastgelegd in kernvragen - wordt vertaald in *Priority Intelligence Requirements* (PIR's).



De inlichtingenorganisatie



### Ook weer en terrein zijn relevant

(Bron: Centrum Audiovisuele Dienstverlening Koninklijke Marine, sectie fotografie)

Deze laatste staan aan de basis van het gehele inlichtingenproces. Binnen de NAVO zijn per strategisch hoofdkwartier deze PIR's uitgewerkt in een strak gestructureerd overzicht van kernvragen en binnen de structuur daarvan afgeleide vragen tot een zeer gedetailleerd niveau. Met de PIR's als basis wordt het verzamelplan opgesteld. Daarmee wordt de behoefte aan inlichtingen gestructureerd naar het gebied en/of het niveau en wordt tevens vastgesteld tot in welk detail dient te worden verzameld.

Het structureren van de behoefte aan inlichtingen wordt uitgevoerd in het *Collection Coordination Intelligence Requirements Management-process* (CCIRM-proces). In dit management-proces worden alle ondergeschikte inlichtingenniveaus opgenomen om

te voorkomen dat verzamelaars verkeerd worden aangestuurd en om te verzekeren dat schaarse, kritische inlichtingenbronnen optimaal worden gebruikt. In het verzamelplan worden alle bronnen van informatie opgenomen. Deze kunnen bestaan uit inlichtingenbronnen van ondergeschikte commandanten, nationale inbreng van de verschillende landen die vertegenwoordigd zijn in zulk een militaire organisatie, open bronnen enzovoort. Het managementsysteem voor verzoeken om informatie (*Request For Information Management System* (RFIMS)) dient ertoe om zo efficiënt mogelijk alle RFI's voor een operatie, via het snelst mogelijke communicatiemiddel te verwerken. De verwerking van informatie van de ondercommandanten en de inlichtingen van de verantwoordelijke commandant

kan ook tot gevolg hebben, dat een aanvullende behoefte aan inlichtingen ontstaat. Afgeleide inlichtingen en doelinformatie zijn in eerste instantie voor gebruik door de verantwoordelijke commandant op operationeel en tactisch niveau, maar de gegevens worden ook ingevoerd voor het ontwikkelen van een *battlefield picture* op strategisch niveau.

### Afhankelijkheid

Omdat de NAVO – los van het *Airborne Warning And Control System* (AWACS) – geen eigen inlichtingenverzamelorganen heeft is zij volledig afhankelijk van de nationale verzamelorganen. Reeds eerder werd gesteld dat de kwaliteit van de inlichtingenanalyses en de inlichtingenproducten, recht evenredig is met de kwaliteit van de ter beschikking gestelde inlichtingen. Indien, om nationale redenen, een deel van de inlichtingen niet ter beschikking wordt gesteld heeft dit rechtstreeks effect op de kwaliteit van de inlichtingenproducten en dus op het advies van de inlichtingenorganisatie aan de commandant. Binnen de NAVO-structuur dient een goede taakverdeling te zijn (*division of labour*) waarbij elk hoofdkwartier zich concentreert op het hem toegewezen gebied van verantwoordelijkheid/belangstelling. Toewijzing van adequaat opgeleid personeel en effectief gebruik van bestaande communicatiemiddelen moet duplicatie van werkzaamheden zoveel mogelijk voorkomen.

Het probleem binnen de NAVO-commandostructuur is echter dat elke commandant geneigd is zijn opdrachten ruim te interpreteren. Daarmee kan een aanzienlijke overlap ontstaan binnen de verschillende verzamelplannen en treedt veelvuldig tijdens het analyseproces duplicatie op. Overigens wordt door de analisten van de verschillende hoofdkwartieren gretig gebruik gemaakt van elkaars analyses en of inlichtingenbronnen. Teneinde de productie van inlichtingen zo veel mogelijk te stroomlijnen

en duplicatie te voorkomen dient gebruik te worden gemaakt van het *Production Management System* (PMS). De opzet van dit systeem is dat door middel van zorgvuldig overleg door alle inlichtingenproductieorganen aan de ene kant 'overkill' moet worden voorkomen en dat aan de andere kant moet worden zeker gesteld dat in het voorzien in de inlichtingenbehoefte geen lacunes ontstaan.

Binnen de NAVO bestaat soms de neiging om het bestaande PMS op een verkeerde wijze te gebruiken. Het gevolg hiervan is dat op het verkeerde niveau inlichtingen worden verzameld en geproduceerd. Een voorbeeld zien we in de praktijk wanneer de inlichtingenorganisaties van *Subordinate Commands* aan strategische analyses werken, en de SC's hun tijd verspillen aan analyses op operationeel en tactisch niveau.

### Het verdere proces

Analyse, integratie en interpretatie van de beschikbare inlichtingen en overige informatie vormen de volgende stap in het inlichtingenproces. Het

is mogelijk dat tijdens dit proces blijkt dat niet alle (gewenste) informatie beschikbaar is of dat informatie van het verkeerde niveau beschikbaar is. Ook kunnen bronnen proberen het inlichtingenproces te frustreren door opzettelijk verkeerde en/of misleidende informatie te geven. Het uiteindelijke product van dit analyse- en integratieproces dient een voorspellende waarde te hebben. Geen enkele commandant is geïnteresseerd in een historisch overzicht van gebeurtenissen. De informatie en inlichtingen dienen hem te vertellen wat hij kan verwachten zodat hij hiermee rekening kan houden bij de uitvoering van zijn opdracht.

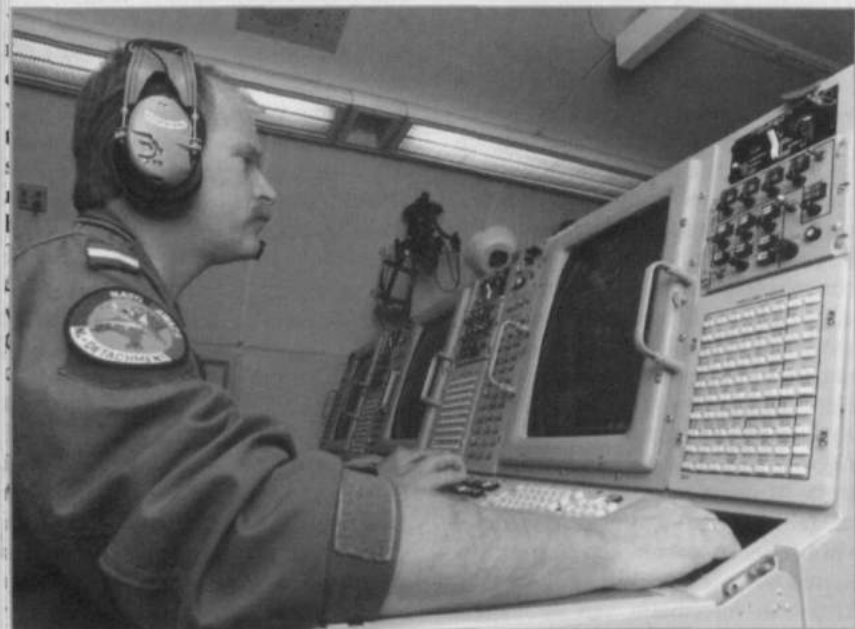
Over het algemeen zijn de geproduceerde analyses binnen de NAVO-inlichtingenorganisatie van hoge kwaliteit. Het blijft een uitdaging om gefundeerde en helder geformuleerde voorspellingen te doen. Toch ligt daarin juist de zin en noodzaak van inlichtingenorganen. Interpreteren en analyseren is een mentaal proces. Het dient onafhankelijk (van de operationele en logistieke secties binnen een staf) te worden uitgevoerd en moet gebaseerd zijn op zo objectief mogelijke bronnen. Het proces moet wor-

den uitgevoerd door officieren en onderofficieren die een zekere mate van ervaring hebben en in staat zijn hun persoonlijk opgebouwde kennis op een juiste en evenwichtige wijze in het analyseproces te gebruiken. Het probleem om personeel met een dergelijke kwaliteit te verwerven is groot, met name bij de kleinere lidstaten, waaronder Nederland. Sommige van deze landen kennen bovendien geen eigen, functiegericht, loopbaanpatroon op inlichtingengebied. Als gevolg van de regelmatige functiewisselingen wordt binnen de inlichtingenorganisaties nauwelijks ervaring opgedaan. De huidige uitzendingen vormen overigens een praktische leerschool, ook voor inlichtingsofficieren.

### Informatiestructuur

De vraag naar informatie en inlichtingen neemt alleen maar toe. Het tijdig beschikbaar hebben van inlichtingen op alle niveaus binnen de NAVO vereist communicatiemiddelen, coördinatie en een informatiestructuur die de verschillende inlichtingennetwerken met elkaar verbindt. Nu nog vormen het (Amerikaanse) LOCE<sup>2</sup> en BICES de door de NAVO meest gebruikte inlichtingensystemen.

BICES is een door zeventien NAVO-landen gedragen systeem dat informatie-uitwisseling verzorgt tussen de deelnemende landen. De informatie kan worden gebruikt voor nationaal, strategisch, operationeel en tactisch niveau. De ontwikkeling van de NAVO-inlichtingeninformatiestructuur wordt in principe geïnitieerd door de gebruiker. De gebruikers eisen het vermogen direct toegang te hebben tot relevante data. Daarbij dient de exploitatie en de verspreiding snel te kunnen plaatsvinden om te voldoen aan de eisen van het besluitvormingsproces.



AWACS: het enige eigen systeem (Bron: foto Hennie Keeris)

<sup>2</sup> LOCE: Linked Operational Intelligence Centre Europe. BICES: Battlefield Information Collection and Exploitation System.

Inlichtingenanalisten moeten in het bezit zijn van geautomatiseerde systemen die gemakkelijk gegevens kunnen opvragen om de voorbereiding en verspreiding van inlichtingenproducten naar andere functionele gebieden (bijvoorbeeld operaties, logistiek) te vergemakkelijken.

Het is van het grootste belang dat flexibiliteit in de informatiestructuur toereikend moet zijn om de verschillen in opdracht en uitvoering te kunnen verwerken. Een belangrijk gevolg hiervan is dat de bestaande informatiesystemen in staat moeten zijn binnen een inlichtingenarchitectuur flexibel te opereren. Tegelijkertijd moet de architectuur zelf flexibel en open genoeg zijn om technologische veranderingen te integreren. Een werkgroep, gevormd door representanten van bestaande netwerken, heeft een – de gehele NAVO omvattende – inlichtingen-netwerkstructuur ontwikkeld, waarbij de bestaande systemen worden gekoppeld en de gebrui-

kers door middel van e-mail en andere faciliteiten toegang verkrijgen tot elkaars gegevens.

In de toekomst geplande en reeds doorgevoerde wijzigingen in de inlichtingen-informatiestructuur zullen er zorg voor dragen dat de *wide area networks* (WAN's), van de NAVO, zoals ACE ACCIS van SHAPE en MCCIS<sup>3</sup> van SACLANT met hun functionele inlichtingentoepassingen gezamenlijk een inlichtingen-informatiestructuur vormen, die alle hoofdkwartieren tijdig kunnen voorzien van de gevraagde informatie. De beschikbare functionele faciliteiten binnen de afzonderlijke informatienetwerken moeten dan voorzien in het gecoördineerd verwerken van onder andere verzoeken om informatie, geografische toepassingen, analyses, archivering, ver-

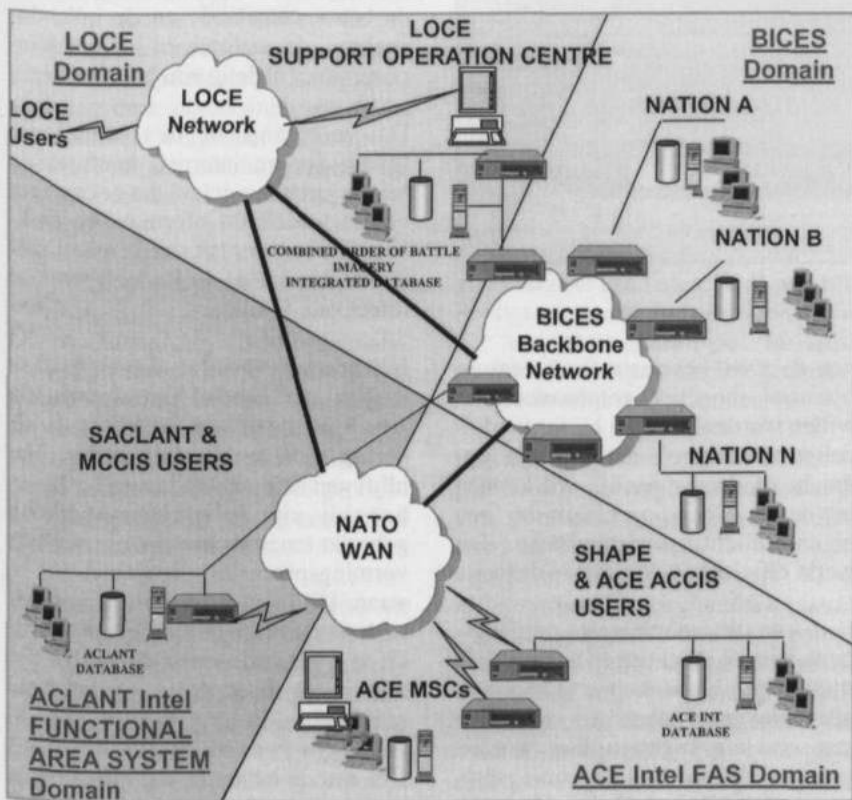
<sup>3</sup> ACCIS: Automated Command, Control and Information System, MCCIS: Maritime Command, Control and Information System.

spreiding en het gebruik van multimediafuncties. Dit is de *near to mid term Integrated NATO Intelligence Architecture*.

## Veranderingen

Na het wegvallen van de grootste, historische dreiging eind jaren tachtig, is een aantal duidelijke veranderingen opgetreden in de inlichtingenwereld; vooral in de beleids sfeer. Allereerst werden de inlichtingenorganisaties verantwoordelijk voor een aanzienlijk groter geografisch gebied. Bovendien moesten zij zich concentreren op een veel groter aantal onderwerpen die een relatie hebben met de aangepaste nieuwe verantwoordelijkheden van commandanten. Zo kregen de inlichtingenorganisaties niet alleen verantwoordelijkheid voor het bestuderen van de zogenaamde artikel-5-scenario's, maar dienden zij zich ook voor te bereiden op twee onafhankelijk van elkaar optredende crisisbeheersingsoperaties (zoals bijvoorbeeld de huidige operaties in Bosnië-Herzegovina/SFOR en in Kosovo/KFOR). Al gauw bleek de bestaande inlichtingenorganisatie grote problemen te hebben met het verzamelen van operationele en tactische inlichtingen. Daarom werd, speciaal voor deze operaties, een eigen inlichtingenorganisatie opgebouwd die tot doel heeft de commandanten die de twee operaties leiden zo goed mogelijk te ondersteunen.

Een andere ingrijpende verandering was het gegeven dat de inlichtingenorganisaties zich moesten concentreren op terreinen die in het recente verleden in het geheel niet door de klassieke inlichtingenorganisaties werden bestudeerd. Werd in het verleden de grootst mogelijke aandacht gegeven aan de slagordeoverzichten van potentiële tegenstanders, nu dienen de inlichtingenorganisaties zich te concentreren op onderwerpen zoals vluchtelingen, fundamentalisme, veiligheid van (civiele) nucleaire installaties, georganiseerde misdaad, proliferatie van massavernietigingswa-



NATO Intelligence Architecture

pens, beschikbaarheid van water en andere voor de bredere veiligheid relevante onderwerpen.

Een volgende omschakeling in de gedachte wereld van de inlichtingen-officier was het ter beschikking komen van kwaliteitsinlichtingen uit open bronnen. Werd in het verleden door de inlichtingenofficier nogal smalend over dit soort bronnen gesproken, inmiddels heeft hij moeten toegeven dat de inlichtingen die hij uit deze bronnen kan krijgen in veel gevallen snel, van hoge kwaliteit en zeer gedetailleerd zijn.



SFOR

### **Aanpassingen**

Inlichtingen dienen relevant, accuraat en objectief te zijn en tijdig ter beschikking te staan. Een gecentraliseerde wijze van werken heeft voordelen. Hierbij is sprake van een integrale analyse gebaseerd op het totaal aan informatie en inlichtingen. Een dergelijke aanpak voorkomt in beginsel duplicatie. Hierover valt binnen de NAVO-context wel het een en ander op te merken.

Over het centraal organiseren van de inlichtingenorganisatie wordt binnen de NAVO-inlichtingenstructuur ver-

schillend gedacht. Binnen de NAVO is er slechts sprake van een centrale behandeling, analyse en verspreiding van inlichtingenproducten in de inlichtingenorganisaties van de staven die de huidige NAVO-operaties van KFOR en SFOR aansturen. In de vredestructuren van de NAVO-hoofdkwartieren is geen sprake van een gecentraliseerde organisatie. Elke commandant binnen de NAVO-bevelsstructuur heeft zijn eigen inlichtingenorganisatie, ontwikkelt zijn eigen commandogereleerde inlichtingenproces en produceert zijn eigen inlichtingenanalyses. Iedere individuele commandant bin-

nen de NAVO-bevelsstructuur zegt zo optimaal mogelijk geïnformeerd te willen worden, waarbij hij ter verduidelijking aangeeft dat hij zijn opdracht zo goed mogelijk wil kunnen uitvoeren. Daarvoor claimt hij een eigen inlichtingenorganisatie. Dit werkt efficiency zeker niet in de hand.

Een van de voornaamste uitgangspunten is dat inlichtingen te allen tijde tijdig beschikbaar dienen te zijn voor alle relevante gebruikers waardoor een cruciale bijdrage kan worden geleverd aan de besluitvormingsprocessen. Dit lijkt voor de hand liggend, maar de praktijk wijst anders uit. Er

zijn namelijk voorbeelden van buitengewoon scherpzinnige en waardevolle inlichtingen, tot op het meest indringende detail uitgewerkt, die te laat ter beschikking van de commandant kwamen en daarmee waardeloos waren.

De ontwikkelingen op het gebied van informatievoorziening zijn in de laatste jaren dusdanig geëvolueerd, dat inlichtingen en informatie razendsnel en in grote hoeveelheden ter beschikking komen. Tegelijkertijd ligt hierin ook een gevaarlijke zwakke schakel. Met het eventueel uitvallen van de communicatiesystemen, al dan niet moedwillig, komt de gehele inlichtingencyclus in gevaar. Ook bestaat de mogelijkheid om informatie moedwillig te manipuleren. Het is technisch gezien relatief eenvoudig elektronisch gemanipuleerde informatie in de communicatiecircuits in te voeren, waarbij bestaande bestanden kunnen worden gemanipuleerd of gewist. Het is duidelijk dat zo'n ontwikkeling een negatieve impact zou hebben die de betrouwbaarheid van de inlichtingenbron, de analisten en het inlichtingenproduct nadelig zou beïnvloeden.

De voortgang in de technologie (onder andere internet) heeft er de laatste jaren toe geleid dat er een zeer grote hoeveelheid informatie beschikbaar is waardoor het steeds moeilijker wordt daaruit de juiste en gewenste informatie te filteren.

Inlichtingenstructuren dienen zorg te dragen dat beschikbare informatie zowel in tijden van vrede, crisis als oorlog tijdig ter beschikking is. Het blijft aan de commandant te beslissen hoe hij zijn inlichtingenmiddelen gebruikt teneinde hem in zijn besluitvormingsprocessen maximaal bij te staan. Hij moet in vredetijd voorbereidingen treffen om in geval van crisis of erger in de kortst mogelijke tijd zijn inlichtingenproces operationeel te krijgen.

Om aan de behoefte aan inlichtingen in tijd van oorlog en/of crisis zo snel mogelijk te kunnen voldoen wordt in

vredes tijd reeds een enorme hoeveelheid inlichtingen in databanken opgeslagen. Tevens worden talloze, zo veel mogelijk de werkelijkheid benaderende plansituaties en inlichtingenanalyses voorbereid en opgeslagen. NAVO's betrokkenheid bij vredesoperaties heeft de vraag naar allesomvattende en relevante inlichtingen sterk doen toenemen.

De NAVO heeft van haar operaties in de Balkan het nodige geleerd. Deze betrokkenheid en de veelal internationaal gewaardeerde uitvoering van de operaties, hebben geleid tot een algehele mondiale analyse van mogelijke crisissituaties waarin de NAVO zou kunnen worden gevraagd op te treden. Tijdens de analyse van deze mogelijke, toekomstige opdrachten is het gehele pakket inlichtingen dat voor, tijdens en na afloop van zo'n mogelijke operatie nodig kan zijn, in beschouwing genomen. Een voorbeeld is de doelenanalyse die na afloop van de bombardementen op Servië werd uitgevoerd. De uitkomst van die doelenanalyse leverde buitengewoon waardevolle informatie op over de mate van succes van de geallieerde bombardementen. De uitkomsten van deze doelenanalyses zullen bij eventueel volgende, toekomstige operaties in de inlichtingenanalyses worden betrokken.

### Enkele bevindingen

De resultaten van inlichtingenanalyses in de voorbereidende fase worden niet alleen ter beschikking gesteld aan de militaire commandanten. Alle beschikbare inlichtingen zullen in eerste instantie mede worden gebruikt ter ondersteuning van preventieve diplomatieke activiteiten.

De huidige operaties van SFOR en KFOR hebben inmiddels een hoeveelheid waardevolle ervaringen opgeleverd. Binnen de inlichtingenstructuren van SFOR en KFOR staan *National Intelligence Cell's* (NIC's) ter beschikking om een maximale coördinatie tussen de NAVO-inlichtingenorganisatie en de nationale inlichtingenorgani-

saties te bevorderen. Een groot aantal landen is door middel van een dergelijke NIC vertegenwoordigd. Het duidelijk zijn dat wederom de landen met de meest robuuste inlichtingenorganisaties het best vertegenwoordigd zijn. Alhoewel deze NIC's voornamelijk het oogmerk hebben de nationale hoofdsteden zo goed mogelijk te informeren is het uiteraard tevens de bedoeling dat de inlichtingenstroom in twee richtingen gaat, waarbij ook de commandant die de operatie leidt zijn voordeel kan halen. In de praktijk huldigt een aantal NIC's de ontvangende 'eenrichtingsstrategie' of kiest ervoor inlichtingen slechts gedeeltelijk ter beschikking te stellen.

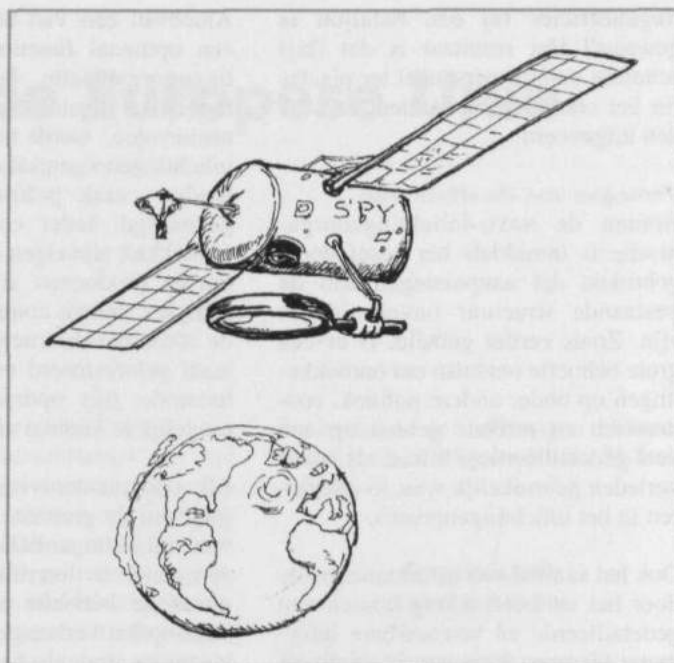
Om aan het verkrijgen van inlichtingen door ondervraging en af luisteren van personen te kunnen voldoen, werd in Bosnië, reeds in het begin van de operatie in 1995, een *Allied Military Intelligence Battalion* (AMIB) opgericht. Inmiddels bestaat de personele bezetting niet alleen uit Amerikanen doch veel NAVO-landen hebben voor deze eenheid personeel ter beschikking gesteld. Een belangrijk deel van de tactische en operationele inlichtingenbehoefte wordt door deze eenheid verzorgd. Discussies over de

verdeling van de kosten om deze eenheid te kunnen laten opereren, heeft de inzetbaarheid van de eenheid negatief beïnvloed (de NAVO kent immers geen eigen eenheden en alleen de VS had een dergelijke eenheid ter beschikking).

### Personeelsproblemen

Een ander probleem is de beschikbaarheid van goed opgeleid inlichtingenpersoneel. De meeste landen hebben grote moeite om de inlichtingenfuncties met goed opgeleid, gekwalificeerd personeel te kunnen vullen. Veel inlichtingspecialisten hebben reeds meerdere rotaties ondergaan en de nationale inlichtingenorganisaties zijn niet in staat aan de vraag naar geschoold inlichtingenpersoneel te voldoen.

Het directe gevolg is dat personeel met een niet of nauwelijks relevante carrièreachtergrond als inlichtingenofficier ter beschikking wordt gesteld. Hij of zij voldoet niet of slechts gedeeltelijk aan de taakomschrijving die bij zo'n inlichtingenfunctie behoort. Hoe vaak gebeurt het niet dat een inlichtingenofficier wordt aangeboden met de kwalificatie dat hij als luitenant twee jaar inlich-



Gezocht...



tingenofficier bij een bataljon is geweest? Het resultaat is dat (bij) scholing van dit personeel ter plaatse (in het operatiegebied) dient te worden uitgevoerd.

#### Verhogen van de effectiviteit

Binnen de NAVO-inlichtingenorganisatie is inmiddels het besef doorgebroken dat aanpassingen aan de bestaande structuur onvermijdelijk zijn. Zoals eerder gemeld, is er een grote behoefte ontstaan om ontwikkelingen op onder andere politiek, economisch en militair gebied op een veel gedetailleerdere schaal als in het verleden gebruikelijk was, te integreren in het inlichtingenproces.

Ook het aanbod van informatie, mede door het ter beschikking komen van gedetailleerde en betrouwbare informatie uit open bronnen, is explosief toegenomen. Vooral door de ervaring die de SC's gedurende de huidige operaties in de Balkan hebben opgedaan, is het gewenst om de effectiviteit van de strategisch/operationele inlichtingen te verbeteren. Ook zal moeten worden bekeken op welke wijze deze nieuwe (open) inlichtingenbronnen kunnen worden geïntegreerd en de ter beschikking staande nieuwe communicatietechnieken beter kunnen worden benut. Hiertoe is de NATO *Intelligence Development Campaign* (NDIC) geïnitieerd. Twee werkgroepen op hoog niveau binnen de NAVO zullen alle inlichtingenactiviteiten opnieuw bezien en zich richten op het doen van aanbevelingen voor het verbeteren van de toekomstige NAVO-inlichtingenorganisatie.

#### Samenvattend

In het voorgaande is getracht een kort, maar zeker niet volledig, overzicht te geven van de problemen en ontwikkelingen binnen de inlichtingenorganisaties van de NAVO.

Alhoewel een van de axioma's van een optimaal functionerende inlichtingenorganisatie, een zo centraal mogelijke organisatiestructuur wordt aanbevolen, wordt binnen de NAVO-inlichtingenorganisaties, om verschillende - vaak politieke redenen - gezondigd. Ieder commandoniveau ontwikkelt zijn eigen inlichtingenproces en produceert zijn inlichtingenanalyses. Iedere commandant binnen de NAVO-bevelsstructuur claimt optimaal geïnformeerd te willen worden teneinde zijn opdrachten zo goed mogelijk te kunnen uitvoeren.

Elk commandoniveau heeft de neiging om de grenzen van zijn gebied van inlichtingenbelangstelling stilzweigend te verruimen. Hierdoor wordt de behoefte aan inlichtingen vaak op het verkeerde niveau gelegd, waardoor strategische commandanten operationele inlichtingen en operationele commandanten strategische inlichtingen gebruiken tijdens hun besluitvormingsprocessen, hetgeen funest is voor een sluitende, strak geëchelonnerde commandovoering.

Als gevolg van een te ruime definitie van de opdrachten aan commandanten, wordt een aanzienlijke overlap van de verzamelplannen gecreëerd. Het gevolg daarvan is een duplicatie van werk, en het niet-economische gebruik van de middelen.

Het *Collection Coordination Requirements Management System* (CCRMS) is een goed functionerend systeem dat slechts gedeeltelijk tegemoet komt aan de eerder genoemde negatieve resultaten van een 'versnipperd' inlichtingentreden.

Er zijn belangrijke verschillen tussen de vroegere en de huidige inlichtingenorganisatie. Allereerst omdat nu een aanzienlijk omvangrijker geografisch gebied en een groter aantal risico's en dreigingen aandacht verdie-

nen. Daarnaast kan er, naast de Artikel 5-inlichtingenbehoefte, een inlichtingenbehoefte voor twee gelijktijdig optredende crisissituaties ontstaan.

Binnen de NAVO-inlichtingenorganisatie is inmiddels het besef doorgedrongen dat aanpassingen aan de bestaande structuur onvermijdelijk zijn. Duidelijk is ook dat de mate van samenwerking vooral wordt bepaald door de feitelijke omstandigheden. Daar waar van gedeelde belangen sprake is gaan eerder gesloten deuren open. Hiertoe is de NATO *Intelligence Development Campaign* (NDIC) geïnitieerd.

De NAVO-landen blijven de voornaamste leverancier van inlichtingen. De verspreidingstechnologie is echter voor de gebruiker van inlichtingen eveneens van wezenlijk belang. De gebruiker van inlichtingen eist snel, accuraat en tijdig informatie. Om dit te bewerkstelligen dienen informatie-technologie en communicatiemiddelen maximaal te worden ingezet. Werd in het verleden veelal informatie collectief aangeboden, de zogenoemde *push*-methode, hedentendage wordt in principe gebruik gemaakt van *pull*-technieken waarbij de gebruiker specifieke inlichtingen aan bronnen onttrekt. De strategische hoofdkwartieren werken samen om de verspreiding van inlichtingen door middel van een geïntegreerde NAVO-inlichtingeninformatiestructuur aanzienlijk te verbeteren.

De boodschap van Generaal Powell is duidelijk. Zij moet leidraad zijn en blijven voor de inlichtingenactiviteiten binnen het bondgenootschap. Inlichtingen vormen het fundament voor besluiten. Daarin ligt dan ook de zin en de noodzaak van inlichtingenorganisaties, ook binnen NAVO.

# Inlichtingen in de Europese Unie

H.A.J. Bokhoven – brigade-generaal\*

## Inleiding

**E**lf juni 2001. *Interim Military Staff* (IMS) wordt *European Union Military Staff* (EUMS). Begonnen in 2000 met niets. Onder het voorzitterschap in Europa van Portugal gegroeid tot vijftien militairen, onder het daaropvolgende Franse voorzitterschap tot dertig en onder het Zweedse tot 64, zal de staf ten tijde van de topconferentie van Laken (december 2001) de voorziene sterkte hebben van 135 personen, afkomstig uit de vijftien lidstaten van de Europese Unie. Op het moment van schrijven (september 2001) zijn reeds 127 militairen binnen. Zonder meer kan gezegd worden dat de lidstaten vaart achter de personele vulling zetten. De officieren en onderofficieren zijn met groot enthousiasme, inzet en deskundigheid gestart om gestalte te geven aan dit Europese initiatief.

Met een omvang van 135 personen – de helft van NAVO's IMS – is de EUMS klein maar fijn.

## Taken

In de door de lidstaten geaccordeerde *Terms of Reference* (TOR) staat onder meer dat de EUMS verantwoordelijk is voor 'early warning, situation assessment and strategic planning for Petersberg tasks ... as directed by the European Union Military Committee

(EUMC)'. Petersbergtaken zijn missies variërend van *humanitarian aid and rescue, peacekeeping* tot en met *peace-enforcement*. Daartoe moet de Europese Unie in 2003 in staat zijn met maximaal 60.000 militairen (en de eraan gekoppelde middelen) gedurende een jaar een operatie uit te voeren.

## Organisatie EUMS

De EUMS heeft een organisatiestructuur die de lezer eenvoudig herkent: *policy/plans, intelligence, operations/exercises, logistics/resources* en *CIS*, georganiseerd in *divisions*. Boven elke *division* staat een *one star* als *assistant chief of staff* (ACOS) (respectievelijk Frankrijk, Nederland, Italië, Spanje en Ierland). Het geheel wordt geleid door de COS, een Britse generaal-majoor. Met boven hem de *director-general*, nu de Duitse luitenant-generaal Rainer Schuwirth. De *divisions* zijn verdeeld in branches, geleid door kolonels; daaronder werken *action officers* (majoor/lkol).

Ter ondersteuning van COS en de *director-general* is er een *Executive Office* (Nederlands geleid). De functies van kolonel en hoger zijn zogenaamde *non-quota* stoelen; met andere woorden deze wisselen naar andere landen. De overige functies zijn vooralsnog vast toebedeelde stoelen. (Bij een toekomstige uitbreiding van de EU zal dit worden herbezien).

Plaatsing is in principe voor de duur van drie jaar, met een (theoretische) mogelijkheid van een verlenging met één jaar. EUMS geeft uitvoering aan

het beleid en de beslissingen overeenkomstig de richtlijnen van het Militair Comité.

## Organisatie EUMS – INT DIV

Zoals hierboven reeds vermeld wordt het *executive office* momenteel Nederlands geleid. Als ACOS heb ik een Nederlandse adjudant-onderofficier als PA/clerk en een civiele secretaresse afkomstig van het Raadssecretariaat.

De divisie is onderverdeeld in drie branches: *Intelligence Policy, Intelligence Requirements* en *Intelligence Production*. *Core business* vindt plaats in de laatste branch, immers daarin zijn de analisten ondergebracht. Voorts is er een *front-end cell* in het *Joint Siten*. Dit *siten* is *joint* omdat hier zowel militairen als diplomaten van de *Policy Unit* (de politiek strategische 'watchdog' van de secretaris-generaal/Hoge Vertegenwoordiger, dr. Solana) samen de situatie in de wereld volgen, beoordelen, briefings voorbereiden etc.

*Intelligence* is de grootste divisie met dertig personen, afkomstig van veertien van de vijftien lidstaten (Luxemburg heeft geen militairen in de INT-divisie).

## Werkwijze

Zoals dit het geval is bij de NAVO, is ook EUMS voor zijn militaire inlichtingen in eerste instantie afhankelijk van de lidstaten. Het is daarom dat de

\* De auteur is Assistent Chief of Staff Intelligence bij de European Union Military Staff.

*Intelligence Division (INT) action officers* heeft die beschikken over een *point to point* beveiligde verbinding met hun nationale militaire inlichtingendienst voor het verkrijgen van bijdragen. Die bijdragen bestaan uit basisinlichtingen, regelmatige INT-SUMS, INTREPS e.d. Voorts zullen we de lidstaten op basis van een specifieke behoefte gerichte vragen stellen. Teneinde de nodige transparantie te verschaffen laten we de lidstaten weten, wie we wat vragen.

De inkomende antwoorden worden door de *Productionbranch* geanalyseerd en verwerkt tot een EUMS-INT *division* product. Dat product wordt intern gebruikt. Afhankelijk van de situatie wordt dit benut om het Militair Comité te brieven en/of dr. Solana. Uiteraard gaat dat product ook naar de (diensten) van de lidstaten. Daar zit toegevoegde waarde voor veel van deze diensten in. Het geheel is meer dan de som der delen. Niet elke lidstaat heeft de capaciteit om elk gebied te volgen. Echter, in voorkomend geval moet zo'n lidstaat wel meebeslissen over het al dan niet uitvoeren van een missie. De verschijningsvorm van onze producten is divers: in de vorm van mondelinge

briefings, al dan niet ondersteund door beelden, in de vorm van *Intelligence Reports* (INTREPS), *Intelligence Summaries* (INTSUMS), *Intelligence Supplementary Reports* (SUPINTREPS). Waar de EU de situatie in de gehele wereld volgt, zijn er prioriteiten gesteld voor bepaalde gebieden/landen. Om heel evidente redenen besteden we eveneens aandacht aan zaken als wapensmokkel, proliferatie en terrorisme.

In de samenwerking met de *Policy Unit*, kunnen in voorkomend geval producten worden gemaakt, die niet alleen de militair-strategische inlichtingen kanten van de medaille belichten, maar ook de politieke kant. De PU krijgt van de lidstaten immers ook diplomatieke rapportages en daarenboven ook rapporten van missies van de EU in de hele wereld. Denkt u maar aan de eigen EU diplomatieke missies en uiteraard de *European Union Monitor Mission* op de Balkan. Dit gezegd zijnde is het wel zo dat de *Intelligence Division* altijd een eigen verantwoordelijkheid houdt en daarmee op basis van eigen analyse zo nodig een afwijkende inschatting van een bepaalde situatie moet (kunnen) geven.

In de voorbereiding en uitvoering van een operatie voorziet EUMS er uiteraard ook in, inlichtingenproducten aan te bieden aan een aan te wijzen/aangewezen operationeel hoofdkwartier (en omgekeerd) en/of een *field HQ* (afhankelijk van de grootte en de aard van de operatie).

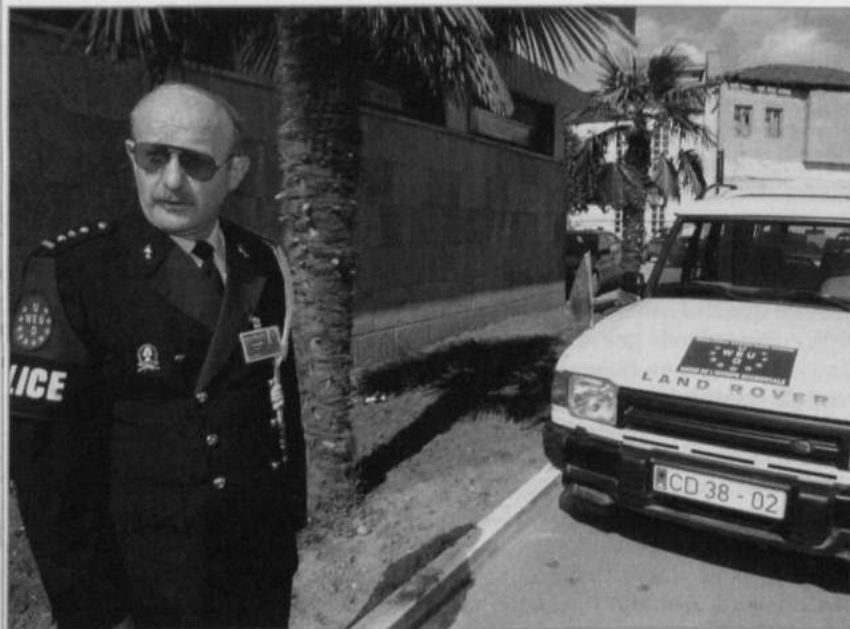
Teneinde in dergelijke situaties slagvaardig te kunnen werken kan EUMS *crisis action teams* instellen, steunend op eigen expertise, personeel en infrastructuur. Voorts kan aan het MC (en dus de lidstaten) verzocht worden extra personeel beschikbaar te stellen. (Het MC van de EU wordt gevormd door de Permanente Militair Vertegenwoordigers van de EU-lidstaten en wordt momenteel voorgezeten door de Finse generaal Gustav Hagglund.) Zoals bekend, is voorzien dat dergelijke operaties ofwel met EU-middelen, dan wel met NAVO-middelen (veelal zijn dat dezelfde, immers elf EU-lidstaten zijn ook NAVO-lid) worden ondersteund/uitgevoerd.

Hiertoe is het van groot belang om - zodra hiertoe politieke goedkeuring is - een nauw contact met de NAVO te onderhouden. Dit geldt voor alle facetten, dus niet alleen inlichtingen. In informele zin zijn deze contacten al gelegd. Dit is uiterst nuttig, omdat we in de EU op militair gebied zoveel als mogelijk dezelfde 'taal' willen spreken als in de NAVO, zeker in operationele sfeer. Heel praktisch kunt u hierbij denken aan onder meer definities/begrippen. Zo worden, dan wel zijn, ook contacten gelegd met UN, OSCE en met (derde) landen.

Ter afsluiting voor wat betreft 'werkwijze', is het nuttig op te merken dat met goede analyses van open bronnen, eveneens wordt bijgedragen aan het maken van inlichtingenproducten.

### Infrastructuur

Sinds mei van dit jaar is de EUMS ondergebracht in een kantoorcomplex aan de Kortenberglaan in Brussel. Samen met het Directoraat-Generaal Externe Relaties, de *Policy Unit* en



Europese inzet

het *Joint Sitcen*. Het gebouw is *up to standards* gebracht qua veiligheidsvoorzieningen. Denk hierbij aan entree, afscherming en verbindingen. Waar elke EU-functionaris kan werken met een *low security LAN* met internetaansluiting, zal dit najaar een *Security Office LAN* (SOLAN; sommigen grappen nu dat er een SOLAN.A is en er een SOLAN.B aankomt) worden geïnstalleerd in de Kortenberg. Voorts krijgt - logischerwijze - de INT-divisie de beschikking over een separaat INT-LAN. Beide netwerken zijn tot en met SECRET gecertificeerd. Deze certificering voldoet ook aan de NAVO-standaard.

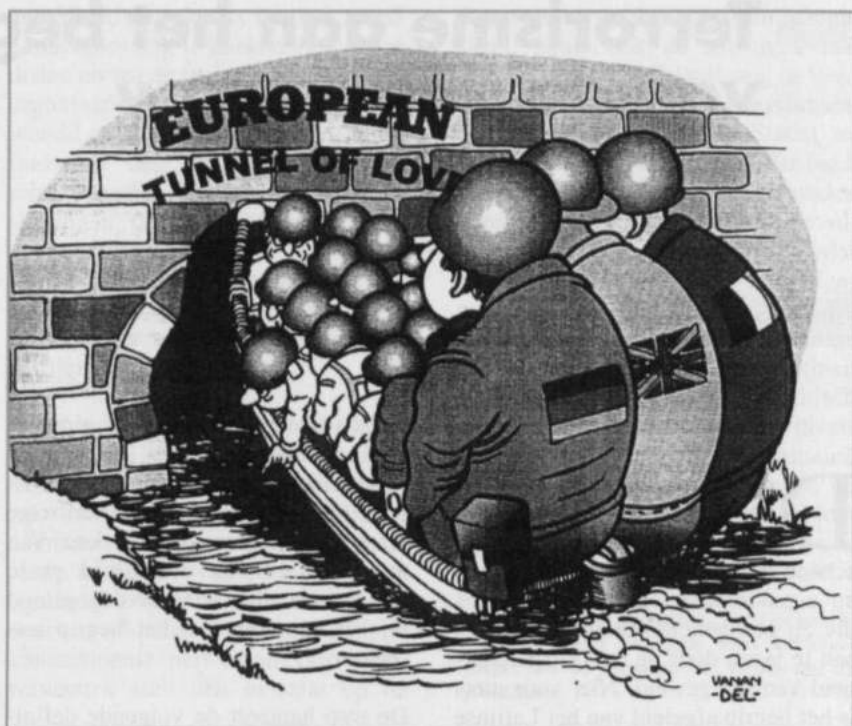
### Observaties

In de EU worden de talen van de lidstaten gerespecteerd. Dit betekent dat waar in de Unie vergaderd wordt over bijvoorbeeld landbouwbeleid, er getolkt en vertaald wordt in onder meer het Nederlands; eenieder spreekt daar zijn eigen taal.

Dat de EUMS, het MC én het *Political and Security Committee* (PSC) alleen Engels en Frans hanteren, zonder tolken/vertalen is a) terecht en b) noodzakelijk. Het waarom behoeft nauwelijks betoog. In een uit te voeren militaire operatie mag letterlijk geen spraakverwarring ontstaan. In EUMS worden alle stukken in het Engels geproduceerd en is de voertaal in feite Engels. In MC en PSC hoort men beide. Nu België het voorzitterschap heeft is de gebezigde taal in het PSC veelal Frans. (Ter vergelijking: in de Noord-Atlantische Raad wordt wel getolkt en vertaald!)

Personeel geplaatst bij EUMS dient Frans en Engels te beheersen. In zijn algemeenheid loopt dat in de dagelijkse praktijk heel behoorlijk.

De militaire structuren van de EU zijn nog heel jong. Nog niet alles is uitgekristalliseerd, dat kost gewoon tijd. Tegelijkertijd is er (politieke) druk op de ketel om sneller dan voorzien tot



'Tunnel of love' (Bron: A.A. van Andel)

actie over te gaan. Maar zo'n actie moet succesvol zijn. Zelfs aan een zogenaamde *low end of the spectrum*-actie zit een groot afbreukrisico. (Destijds was de UN-missie in Somalië een humanitaire operatie; we weten hoe dat uiteindelijk is afgelopen...). Dat kunnen we ons niet veroorloven. In een vergelijking: sommigen willen dat we meedoen aan de Olympische Spelen, maar we zijn nog maar net in het stadium dat we kunnen lopen. Derhalve is het van eminent belang dat vastgehouden wordt aan de mijlpalen, waarvan het jaar 2003 - zoals beschreven onder het kopje 'taken' - de belangrijkste is.

### Tot slot

Een nieuwe loot in de inlichtingengemeenschap is gegroeid en groeide in Brussel. Staatshoofden/regeringsleiders van de EU-lidstaten besloten hier ten principale toe op de top van Helsinki in 1999, toen ze geza-

menlijk besloten dat nieuwe permanente en militaire instanties zouden worden opgezet, om de EU in staat te stellen haar verantwoordelijkheid op te nemen voor het geheel van taken op het gebied van conflictpreventie en crisisbeheersing als omschreven in het Verdrag van de EU, de zogenaamde Petersbergtaken.

Een uiterst boeiende en interessante situatie, waaraan ook Nederlandse officieren en onderofficieren (momenteel elf van KM, KL en KLU in de EUMS, daarvan vier in INTEL) met veel enthousiasme hun bijdrage leveren. Weliswaar is er over Europese initiatieven veel gezegd en gepubliceerd, ook in defensiebladen, toch is er nog niet zoveel over bekend bij de gemiddelde militair.

Welnu, u kunt als geïnteresseerde - in een verloren moment? - uiteraard terecht op de sites van de EU, met name die van de Raad van de Europese Unie (waaronder EUMS valt); [www.ue.eu.int](http://www.ue.eu.int).

# Terrorisme aan het begin van de 21ste eeuw

drs. E.S.M. Akerboom\*

## Inleiding

De kracht van het terrorisme als politiek wapen ligt eigenlijk niet zozeer in de feitelijke schade die zij aanricht aan personen en eigendommen, maar in de vrees die zij een gehele samenleving weet aan te jagen door de onvoorspelbaarheid van het geweld. Niet voor niets is het begrip afgeleid van het Latijnse woord voor angst (terror). Dat de impact van terrorisme per definitie de feitelijke schade overtreft, verklaart waarom de bestrijding en voorkoming van dit fenomeen nationaal en internationaal voortdurend hoog op de politieke agenda staat, ook in tijden waarin de actuele dreiging op het eerste oog wat minder lijkt.

## Definitie

Er bestaat – ook in de wereld van inlichtingen- en veiligheidsdiensten – geen eenduidige definitie van het begrip terrorisme. Het gebruik of juist het bewust achterwege laten van de term terrorisme, is veelal ook een politieke keuze.

Bij de BVD wordt reeds jarenlang gewerkt met een 'smalle' definitie van terrorisme. Hieraan ligt een bewuste keuze ten grondslag, die zijn oorsprong vindt in de gebeurtenissen van de jaren zeventig in diverse Europese landen. De ervaringen uit die tijd hebben geleerd dat het tot ter-

rorist verklaren van politiek geweld-dadige activisten, met de daarbij behorende *overkill* van justitiële en politieke maatregelen, in ernstige mate radicaliserend kan werken. Van BVD-zijde is dan ook altijd grote terughoudendheid aan de dag gelegd bij het hanteren van het begrip terrorisme.

De BVD hanteert de volgende definitie: *terrorisme is het plegen van of dreigen met op mensenlevens gericht geweld, met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden*. Het vanuit politieke motieven veroorzaken van zaakschade, ook al is deze omvangrijk, of het ontregelen van het maatschappelijk leven kan weliswaar worden beschouwd als een ernstige aantasting van de democratische rechtsorde, maar wordt op grond van de gehanteerde definitie niet aangeduid als terrorisme. Dergelijke activiteiten zijn wel degelijk bedreigend voor de democratische rechtsorde, maar worden door de BVD onderzocht onder de noemer politiek gewelddadig activisme.

## Rechtsgronden

Terrorisme als zodanig wordt niet gedefinieerd in de Nederlandse wetgeving. Anders dan in veel andere landen kan hier dan ook niemand veroordeeld worden voor lidmaatschap van een terroristische organisatie of het plegen van terroristische aanslagen. Verdachten in deze sfeer worden vervolgd voor criminele handelingen

die gebruikelijk zijn bij terroristen, zoals het in gijzeling nemen van personen, huisvredebreuk, doodslag of moord. Ook biedt artikel 140 van het Wetboek van Strafrecht de mogelijkheid een groep te bestempelen als een criminele organisatie, waarvan het lidmaatschap strafbaar is. Toch wordt terrorisme ook in Nederland allerm minst beschouwd als een eenvoudig geweldsdelict. De politieke motivatie van de daders en de evidente dreiging die ervan uitgaat voor het functioneren van de democratische rechtsorde, maken dat op basis van de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) bij de BVD een zware verantwoordelijkheid en dito middelen zijn neergelegd om terroristische activiteiten te helpen voorkomen.

Terrorisme wordt al sedert de jaren zeventig wereldwijd gezien als een van de belangrijkste bedreigingen voor de internationale rechtsorde. De bestrijding ervan heeft dan ook een hoge prioriteit binnen diverse internationale overleggen. Nederland heeft zich daarbij via de ondertekening en ratificatie van VN-verdragen, uitspraken van het Internationaal Gerechtshof en door afspraken in EU- en NAVO-verband, op uiteenlopende niveaus gecommitteerd aan het leveren van een bijdrage aan het tegengaan van terrorisme.

## De actuele dreiging internationaal

Separatisme en islamisme kleuren aan het begin van de eenentwintigste

\* De auteur is directeur Democratische Rechtsorde bij de Binnenlandse Veiligheidsdienst (BVD).

eeuw nog steeds het internationale dreigingsbeeld van de terrorismebe-strijders. Hoopvolle ontwikkelingen aan het diplomatiek front, die duiden in de richting van vreedzame oplossingen voor aloude terroristische broedplaatsen in het Midden-Oosten, Noord-Ierland, Baskenland en Turkije, zijn voor een deel weer afgebroken of in een gevaarlijke impasse geraakt. Het vredesproces in het Midden-Oosten lijkt alleen in naam nog te bestaan, waardoor de frustraties aan beide zijden zich opstapelen. In Noord-Ierland is het een reëel gevaar gebleken dat radicale splinters het broze bestand met geweld zullen breken. In Spanje heeft de ETA, na het stopzetten van besprekingen over een politieke oplossing van de Baskische kwestie, de strijd in alle hevigheid hervat met moordaanslagen op politici en militairen. De Turkse overheid hecht geen enkel geloof aan de

bereidheid van de PKK om een vreedzame oplossing te zoeken voor Koerdistan en zet de jacht op leden van de organisatie onverdroten voort. De wereld zal daarom ook in de nabije toekomst nog herhaaldelijk opgeschrikt worden door terroristische aanslagen in deze sferen, waarbij de doelwitten als voorheen hoofdzakelijk gezocht zullen worden in de conflictgebieden zelf en te relateren zullen zijn aan de elkaar bestrijdende partijen.

Wereldwijd is de dreiging die uitgaat van het religieus geïnspireerd terrorisme, met name gepleegd door radicale moslims, eveneens ernstig te noemen. De voorspelbaarheid van plaats en doelwit van deze terroristen is minder groot. De bestaande grensoverschrijdende contacten binnen transnationale netwerken van geestverwanten stelt hen in staat op de

meest onverwachte plaatsen toe te slaan, zoals ook de inwoners van Nairobi en Dar es Salaam nog in 1998 tot hun schade hebben ondervonden. Met name de Verenigde Staten en Israël, maar recentelijk ook Rusland, worden verantwoordelijk gehouden voor het lijden van de moslimbevolking en weten zich doelwit van islamitische extremisten. In zijn algemeenheid heeft het *jihaddisme*, dat wil zeggen het voeren van een heilige oorlog tegen alle heidense machten en het streven naar een islamitisch wereldkalifaat, een belangrijke plaats in het denken van dergelijke fanatici, hetgeen in uiteenlopende kringen de drijfveer kan vormen voor gewelddadige acties tegen westerse doelen.<sup>1</sup>

<sup>1</sup> Op 11 september jongstleden heeft de wereld op nooit eerder vertoonde wijze kennisgemaakt met de verwoestende kracht van dit *jihaddisme*.



**Geloof en terreur: inspiratie, dwaling, etiket of schaamlap?** (Bron: abc-press)

Het risico dat bepaalde staten steun of sturing geven aan terroristische organisaties, is de afgelopen jaren daarentegen afgenomen. Landen als Syrië, Libië, Iran en Soedan zijn door de Verenigde Staten – en in navolging daarvan door een groot deel van de internationale gemeenschap – regelmatig beschuldigd vanwege hun steun aan het terrorisme. De internationale verontwaardiging over deze staatshulp en de op basis daarvan opgelegde sancties, hebben er mede toe bijgedragen dat de regeringen van deze landen zeer voorzichtig en terughoudend zijn geworden bij hun steunverlening. Libië, dat sedert de explosie van het Pan Am-vliegtuig boven Lockerbie al in het internationale beklagdenbankje zit, heeft er alles aan gedaan om de internationale gemeenschap te overtuigen van zijn goede bedoelingen. Soedan heeft als gevolg van deze druk menige terrorist het land uitgezet, onder wie de beruchte Carlos en Osama bin Laden. Syrië weigerde nog langer onderdak te bieden aan PKK-leider Öcalan. De terrorisme-ondersteuning vanuit deze landen heeft door dit alles aanmerkelijk aan belang ingeboet.

Tegenover het afnemende risico van staatsondersteuning aan terrorisme staat het gevaar dat terroristische groepen hun domicilie of uitvalsbasis kiezen in zogeheten *failed states*. Dit zijn staten waar feitelijk sprake is van anarchie of de afwezigheid van een functionerend overheidsgezag. De overheden in deze landen geven weliswaar geen actieve steun aan dergelijke terroristen, maar zijn evenmin in staat hun aanwezigheid of activiteiten effectief tegen te gaan. In het verleden was Libanon zo'n broedplaats van internationaal terrorisme. Risicolan-

den zijn hedentendage onder meer Afghanistan – waar Bin Laden zijn toevlucht heeft gezocht – Somalië en diverse voormalige Sovjetstaten. Ook sommige staten in zwart-Afrika lopen het risico zich in deze richting te ontwikkelen.

Met het ontstaan van het Osama bin Laden-netwerk en andere terroristische organisaties van islamitische signatuur, heeft het terrorisme in het laatste decennium van de twintigste eeuw een duidelijk andere dimensie gekregen. Was er in het verleden meestal sprake van een min of meer directe relatie tussen slachtoffers en het politieke doel van de terroristen, deze relatie lijkt steeds meer van ondergeschikt belang te worden. Hoewel de Amerikaanse ambassades doelwit waren van de bommenleggers in Afrika, vielen veruit de meeste doden onder de lokale bevolking. Als religieuze fanatici deerde het de daders van de aanslag blijkbaar weinig dat nota bene vooral (moslim) geloofsgenoten het slachtoffer werden, omdat in hun ogen het hogere (goddelijke) doel deze zware middelen heiligt. Een-zelfde legitimatie voor ongebreideld geweld valt waar te nemen bij de Algerijnse GIA en een afsplitsing daarvan, de GSPC, die nu al ruim acht jaar dood en verderf zaait onder de eigen bevolking.

Een dergelijke vorm van niets of niemand ontziend terrorisme is tot op heden hoofdzakelijk toe te schrijven aan religieus geïnspireerde groeperingen. Het zijn vooral organisaties van islamitische signatuur die blijk hebben gegeven van de bereidheid hier toe. Van tijd tot tijd zijn er echter aanwijzingen dat ook bij sommige 'fundamentalistische' en 'sektarische' bewegingen binnen andere religies, het opofferen van mensenlevens voor een hoger goddelijk doel gesanctioneerd wordt. Te denken valt bijvoorbeeld aan de aanslag met het gifgas *sarin* op de metro van Tokio, die in 1995 gepleegd werd door de Japanse Aum Shinri Kyo-sekte. Acties als deze lijken de veel geciteerde stelling van de Amerikaanse terrorisme-

expert Brian Jenkins te logenstraffen, die van mening is dat terroristen er vooral op uit zijn om veel mensen toe te laten kijken en te laten luisteren en niet om veel mensen te doden. Volgens hem willen terroristen slechts zoveel mensen doden als noodzakelijk voor het bereiken van hun politieke doeleinden.<sup>2</sup>

De vraag dringt zich dan ook op of de wereld thans moet vrezen voor een toename van buitenzinnig of redeloos geweld door religieuze extremisten. Bij alle gruwelijke details moet vastgesteld worden dat, afgezien van de gifgasaanval in Tokio en de massale slachtingen in Algerije, er nog immer een zekere correlatie bestaat tussen de 'uitgekozen' slachtoffers en het beoogde politieke doel.<sup>3</sup> De genoemde uitzonderingen tonen echter aan, dat met name bij religieuze fanatici in potentie een risico bestaat dat op dit vlak een vervaging zal optreden, of dat vanuit een *jihad*-gedachte of een vorm van eindtijddenken ('Armageddon') een bereidheid kan ontstaan om met een grote mate van willekeur zoveel mogelijk slachtoffers te maken. Zorgwekkend in dit verband is de aanhouding in december 2000 door de Duitse politie van een groep Noord-Afrikanen met een Afghanistanconnectie, die een gedetailleerd plan hadden opgesteld om een fragmentatiebom tot ontploffing te brengen op een massaal bezochte kerstmarkt in het Franse Straatsburg. Deze zaak maakt duidelijk dat ook Europa zich niet gevrijwaard mag weten van dergelijke vormen van terrorisme.<sup>4</sup>

Wat betreft de mogelijkheden voor terroristen om een groter aantal slachtoffers te maken zal overigens veel afhangen van de technologische ontwikkelingen. Met de huidige 'conventionele' middelen kan de terrorist weliswaar groot leed veroorzaken, doch zijn slachtofferpotentieel blijft relatief beperkt. Nieuwe wapens in de sfeer van de nucleaire, biologische en chemische (NBC-)technologie zouden een aanmerkelijk groter 'bereik' kunnen hebben. De vraag is echter hoe groot het risico is dat dergelijke

<sup>2</sup> B.J. Jenkins, *The likelihood of nuclear terrorism*, Sancta Monica 1985, p.6.

<sup>3</sup> M. van Leeuwen, *Religieus terrorisme als 'nieuwe dreiging'*, in: *Internationale Spectator* 1999, p. 601.

<sup>4</sup> Het terroristische netwerk van radicale moslims, dat in september 2001 in onder meer Rotterdam is opgerold, vormt opnieuw een bewijs voor deze stelling.

wapens gaan behoren tot het arsenaal van de terrorist van de toekomst.

Het leggen van 'conventionele' bommen zal echter hoe dan ook tot het favoriete repertoire van de moderne terrorist behoren. Politieke ontvoeringen, zoals in de tijd van de Rode Brigades (Aldo Moro) en de RAF (Hans-Martin Schleyer), komen in het Westen weinig meer voor, maar vormen elders (Colombia, Filippijnen) nog steeds een lucratieve manier om de 'oorlogskas' te spekken. Ook het oude middel van vliegtuigkapingen heeft in de loop der tijd sterk aan betekenis verloren, mede als gevolg van de verscherpte beveiliging op internationale luchthavens.<sup>5</sup> Het risico dat terroristen binnen afzienbare termijn kunnen beschikken over effectieve chemische, nucleaire, biologische of radiologische (CNBR-) wapens of andersoortige geavanceerde strijdmiddelen moet vooralsnog als gering worden ingeschat, maar wordt internationaal niet genegeerd vanwege de ingrijpende consequenties indien zo'n ontwikkeling zich onverhoopt toch zou voordoen.<sup>6</sup>

Op de middellange termijn zijn er verschillende risico's te duiden die voeding kunnen geven aan terrorisme. Bovenal valt daarbij te denken aan de demografische ontwikkelingen in de Derde Wereldlanden in combinatie met een achterblijvend demo-



**Onschuldige slachtoffers** (Bron: abc-press)

cratiseringsproces, en te geringe economische groei en toenemende schaarste (water!). Een omvangrijke nieuwe generatie zal worden geblokkeerd in haar toekomstperspectieven en een uitlaatklep zoeken voor haar frustraties. Deze ontwikkeling kan aanleiding geven tot het ontstaan van gewapend verzet in de betreffende landen, maar evenzeer leiden tot *braindrain* naar rijke landen. Indien ook daar de perspectieven van de migranten slecht blijken te zijn, kan dat evenzeer voeding geven aan het ontstaan van gewelddadige oppositie. De ontvankelijkheid voor radicale ideologieën met simpele oplossingen voor gecompliceerde problemen - zoals het islamisme, nieuwe religieuze bewegingen (sektes) of het rechts-extremisme - zal in die situatie ongetwijfeld groter worden en daarmee kan een voedingsbodem ontstaan voor nieuwe terroristische erupties.

### **De actuele dreiging voor Nederland**

De terroristische dreiging voor Nederland is voor het grootste gedeel-

te een afgeleide van de internationale dreiging. Indien Amerikaanse of Israëliëse belangen zich in het vizier bevinden van terroristen, lopen zij ook in Nederland gevaar. Hetzelfde geldt voor vestigingen en eigendommen die in verband gebracht kunnen worden met landen die te kampen hebben met separatistisch of andersoortig terroristisch geweld, zoals Groot-Brittannië of Turkije. De internationalisering van het terrorisme heeft er immers toe geleid dat politieke geweldsplegers in principe overal ter wereld kunnen toeslaan, ook in Nederland. Bij dit alles mag niet veronachtzaamd worden dat er verschillende omstandigheden zijn die Nederland in potentie aantrekkelijk maken voor terroristen, hetzij om zich er schuil te houden of om de logistiek te regelen.

Allereerst is er de geografische factor. Nederland ligt op een knooppunt van internationale verbindingen en beschikt over een uitstekende infrastructuur. Zelfs strenge beveiliging kan waarschijnlijk niet voorkomen dat internationaal opererende terroristische organisaties gebruikmaken van

<sup>5</sup> De daders van de aanslagen in New York en Washington confronteerden de wereld met een geheel nieuw fenomeen. Vliegtuigen werden niet gekaapt om via gijzeling politieke concessies af te dwingen, maar veranderden in handen van de kapers tot moorddadige wapens. Feilloos wisten de kapers daarbij de strengere internationale beveiliging te omzeilen door te kiezen voor binnenlandse lijnvluchten in de Verenigde Staten.

<sup>6</sup> De jongste aanslagen in de VS roepen de vraag op of veronderstelde barrières tegen het gebruik van dergelijke wapens nog evenveel opgeld doen. De psychische drempel om dergelijke afschuwelijke middelen te gebruiken lijkt thans in elk geval verlaagd. Blijft staan de vraag in welke mate terroristen inmiddels over de benodigde technische middelen en kennis voor het gebruik van dergelijke wapens beschikken. Overigens is nog eens gebleken dat het ook zonder gebruikmaking van CNBR-wapens mogelijk is, onvoorstelbare schade aan te richten.



de Nederlandse infrastructuur om bijvoorbeeld wapens te verzenden, geld door te sluisen of personen te smokkelen.

Kwetsbaar is Nederland ook als gevolg van zijn politieke ambities en verplichtingen op het internationale vlak. Opeenvolgende kabinetten hebben ernaar gestreefd Nederland wereldwijd een positie te geven als gastheer van internationale gerechts-hoven en toezichthoudende organen. Dat deze positie tevens een zeker risico van aanslagen met zich meebrengt, zal ook in de toekomst moeten worden ingecalculiseerd en stelt hoge eisen aan de beveiliging.

Een derde risicofactor voor Nederland als het gaat om terroristisch geweld, vormt de mogelijke import van gewelddadige conflicten. De grootschalige migratiebewegingen van de afgelopen decennia hebben ertoe geleid, dat groepen van verschillende nationaliteit en etnische afkomst hier hun domicilie gezocht hebben. De bestaande tegenstellingen worden door migranten als het ware geïmporteerd naar Nederland en er moet rekening mee worden gehouden dat dergelijke conflicten in het slechtste geval ook hier tot geweldsuitbarstingen kunnen leiden.

Een laatste risico voor Nederland vormt het eigen juridische en politiek-maatschappelijke klimaat. Internationaal geniet ons land een zekere faam, dan wel treft het blaam vanwege een milde strafoplegging en een grote mate van tolerantie ten opzichte van politieke of religieuze opvattingen onder de eigen, maar ook onder nieuw ingekomen bevolkingsgroepen. Gebleken is dat dit beeld van Nederland niet alleen van tijd tot tijd leidt tot kritiek van sommige landen over de vrijheid die geboden wordt aan in hun ogen extremistische of zelfs terroristische organisaties, maar dat er ook een zekere aantrekkingskracht van uitgaat op personen met terroristische antecedenten. Op voorhand kan niet geheel uitgesloten worden dat zij zich onder omstandighe-



Osama bin Laden (Bron: abc-press)

den ook zullen richten op doelen in het gastland, in casu Nederland.

Bij al deze factoren gaat het in principe om een terroristische dreiging die van buitenaf op Nederland afkomt. Resteert de vraag of ook binnen de Nederlandse samenleving een voedingsbodem bestaat voor het ontstaan van terrorisme. Anders dan in de meeste omliggende landen hebben vormen van *homegrown* terrorisme geen actuele betekenis. Voor de wat langere termijn mag de mogelijkheid evenwel niet op voorhand uitgesloten worden, dat een onverhoopt tot werkelijkheid wordende maatschappelijke tweedeling langs etnische scheidslijnen frustraties oplevert, die een voedingsbodem kunnen vormen voor radicalisme en extremisme. Een zeker continuüm tussen mislukkende integratie, versterkte segregatie, toenemende polarisatie en gewelddadige confrontatie is zeker voorstelbaar, al zijn er absoluut geen indicaties dat een dergelijke ontwikkeling in Nederland uiteindelijk zou kunnen resulteren in het zwartste scenario, dat van het terrorisme.

Over het geheel genomen kan geconcludeerd worden dat er bij het ingaan van de eenentwintigste eeuw geen sprake is van een groot risico dat de samenleving binnen afzienbare termijn geconfronteerd zal worden met terroristische aanslagen op Nederlands grondgebied. Toch zijn er voldoende risicofactoren die waakzaamheid vereisen. Nederland mag zich er dan op verheugen geen belangrijk terroristisch doelwit te zijn, als logistiek knooppunt en als – al dan niet tijdelijke – verblijfplaats van terroristen heeft het onmiskenbaar aantrekkingskracht.

### Conclusie

De BVD heeft op grond van zijn wettelijke taakstelling, expertise, informatiepositie, nationale en internationale relatienetwerk en inbreng in de internationale contra-terrorisme (CT)-fora, vanouds in Nederland een vooraanstaande rol bij terrorismebestrijding. Omdat te voorzien is dat het verschijnsel terrorisme, ondanks ingrijpende veranderingen in de politieke context, ook de komende tijd een belangrijke bedreiging zal vormen voor de nationale en internationale veiligheid, zal deze taak niet snel aan belang inboeten. Wel is een verschuiving in het karakter van de BVD-inzet waar te nemen. Waar vroeger het accent lag op onzekerheidsreductie in de Nederlandse context, zal de aandacht in de toekomst eveneens moeten uitgaan naar preventie en ondersteuning in het bredere kader van de internationale strijd tegen het terrorisme, een verschijnsel dat in principe op elk onverwacht moment en overal ter wereld, Nederland niet uitgezonderd, kan toeslaan.<sup>7</sup>

<sup>7</sup> Deze bijdrage is een samenvatting van het BVD-rapport *Terrorisme aan het begin van de 21e eeuw; dreigingsbeeld en positionering BVD* van april 2001. In enkele voetnoten wordt gewezen op de situatie na de recente aanslagen in de Verenigde Staten. De volledige tekst van de notitie is op aanvraag verkrijgbaar bij de BVD, postbus 20010, 2500 EA Den Haag, of via de website van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties op [www.minbzk.nl](http://www.minbzk.nl)

# Biologische wapens

## Minuscuul wapen met grote gevolgen

drs. S. Stienstra – luitenant-ter-zee 2OC\*

**M**ilitante terroristen blijken interesse te krijgen voor de biologie. Het is echter niet het groen in de natuur, maar de wonderlijke wereld van de microbiologie die hen aantrekt. Bacteriën en virussen, die de mens ziek kunnen maken, hebben de belangstelling gekregen. Met moderne biotechnologische technieken kunnen de micro-organismen nieuwe eigenschappen krijgen, waardoor de getroffen nog zeker wordt of er zelfs zeer snel aan kan sterven.

Vooraf in Amerika voelt men de dreiging. In de vergadering van 18 juli 2001 van de Subcommissie Nationale Veiligheid van de Amerikaanse Senaat rapporteerde FBI-agent Brian Underwood, dat de laatste drie jaren het aantal bioterroristische dreigingen boven de honderd per jaar is gestegen. Alle dreigingen bleken vals, maar de Amerikaanse regering bereidt zich serieus voor op echte aanvallen. Bij de laatste oefening onder de code-naam *Dark Winter* bleek dat de voorbereidingen en voorzieningen om een bioterroristische aanslag te verijdelen of de gevolgen te beperken, nog volstrekt onvoldoende zijn. De oefening van 22 tot 23 juni 2001 op *Andrews Air Force Base* in Washington D.C., maakte duidelijk dat door gebrekkige communicatie, moeilijke diagnose bij de slachtoffers, te weinig detectiemogelijkheden voor het agens en een gebrek aan vaccins het nog onmogelijk is om rampen te voorkomen.

De *National Guard* kreeg al eerder, in maart 1988, van defensie-minister William Cohen opdracht om een antwoord te vinden op chemische en biologische terroristische aanvallen. Tien snel inzetbare *Rapid Assessment and Initial Detection (RAID)* teams, die nu *Civil Support Teams (CST)* heten, werden opgezet om zowel overheid als lokale bevolking en de gezondheidsdiensten te assisteren bij een dergelijke aanval. De uiteindelijke coördinatie bij bioterroristische aanvallen op de burgerbevolking heeft president Bush recent bij het ministerie van Volksgezondheid gelegd en in het bijzonder bij de *Federal Emergency Management Agency (FEMA)*. Uiteraard bestaat er een intensieve militair

civiele samenwerking. Het is echter nog niet voldoende. President Bush heeft op 8 mei 2001 verklaard dat er in oktober 2001 een nieuw rapport beschikbaar moet zijn over de weerbaarheid van de Verenigde Staten tegen bioterroristische aanvallen en hij gaf de directeur van de FEMA, Joe Allbaugh, de opdracht om een nationaal bureau in te richten dat bij bioterroristische calamiteiten direct de coördinatie op zich kan nemen. Het beschikbare budget is dit jaar 348 miljoen dollar.

Getuige het advies van de Gezondheidsraad van 14 juni 2001 aan minister Borst, begint ook in Nederland het besef door te breken dat iets aan deze



Oefenen onder NBC-omstandigheden

\* De auteur is specialist op het gebied van biologische oorlogvoering. E-mailadres: stef.stienstra @ inter.nl.net

nieuwe dreiging gedaan moet worden. De Gezondheidsraad stelt voor om onder auspiciën van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een draaiboek 'Bioterrorisme' op te stellen en dit te beproeven via regelmatige en goed georganiseerde oefeningen. De plaats van defensie en de omvang van het budget zijn overigens nog onduidelijk.

### Wat zijn biologische wapens?

Het begrip biologische wapens omvat alle ziekmakende organismen of giftige stoffen, die in de natuur voorkomen, en gericht op mensen, dieren of planten kunnen worden gebruikt om deze te verwonden (ziek te maken) of te doden. Het is al een oud wapen: de gifpijl, het werpen van lijken in waterbronnen en het moedwillig besmetten van tegenstanders met ziektekiemen, zijn allen vormen van biologische oorlogsvoering. Inzet van biologische wapens bij oorlogen tussen landen wordt niet zo groot geacht, maar de dreiging van het gebruik van deze middelen door terroristische groepen des te meer. Terroristen kunnen het wapen relatief gemakkelijk produceren. De receptuur kan men op het internet vinden. Deze dreiging is zeer groot omdat biologische wapens onzichtbaar zijn, de slachtoffers niet te selecteren zijn en afweer niet gemakkelijk is. Weglopen is vrijwel onmogelijk en eenmaal besmet betekent dat bij een aantal biologische wapens een gewisse dood op een gruwelijke wijze.

Dat ziekten van verre kunnen aanwaaien, kennen we van de recente mond- en klauwzeer (MKZ) epidemie. Soms hebben auto's 's nachts een laagje stofzand gekregen. Dit is zand uit de Sahara, dat in stofwolken lange afstanden overbrugt. Satellietbeelden van 13 februari 2001 tonen zo'n Sahara stofwolk die naar Groot-Brittannië dreef. Een week later, de incubatietijd van MKZ, brak het mond- en klauwzeer ter plaatse uit. In de Sahara is de ziekte endemisch en de



**Veel praktische problemen**

kiemen kunnen gemakkelijk met het zand meeliften. De hypothese is nog niet bewezen, maar de Amerikaanse geoloog Dale Griffin vindt het meer dan toevallig.

### Geschiedenis

Het biologische wapen gaat terug tot de oudheid. Scythische strijders doopten hun pijlen in de rottende lijken van gesneuvelde soldaten om hun thuisland aan de Zwarte Zee te verdedigen tegen aanvallen vanuit de buurlanden. Perzische, Griekse en Romeinse oorlogsverhalen spreken over het gooien van kadavers in waterbronnen en de overwinning van de Tataren op Kappa was te danken aan het slingeren van lijken naar de belegerde stad om aldaar de pest te verspreiden.

Eeuwen later deden de Russen dit opnieuw toen zij in 1710 de stad Reval, in Estland, op de Zweden wilden veroveren. Zij katapulteerden slachtoffers van de toen heersende pest over de stadsmuren.

Tijdens de *French and Indian War* (1754-1763) gaven Britse troepen in Noord-Amerika dekens, die afkomstig waren van patiënten met mazelen, aan Indianen. De in Amerika onbekende ziekte was dodelijk voor

de lokale bevolking, terwijl de Britse strijders immuun waren voor de kinderziekte. In feite een slim staaltje etnische oorlogsvoering. Het verwerpelijke gebruik van biologische wapens beperkt zich in de geschiedenis niet tot ziekmakende micro-organismen. Het meest fantastische verhaal komt uit de Romeinse tijd, waarin Hannibal in een zeeoorlog in het jaar 190 voor Christus, Eumenes II, de koning van Pergamen, overwon door aarden potten met giftige slangen op de vijandelijke schepen af te vuren.

In de vorige eeuw werd als gevolg van de bloei van de Duitse biochemie en microbiologie, aan het einde van de negentiende eeuw professioneel gewerkt aan biologische strijdmiddelen. Gedurende de Eerste Wereldoorlog ontwikkelden de Duitsers als biologisch wapen anthrax (miltvuur), kwade droes (een paardenziekte), cholera en een schimmel om tarweoogsten te vernietigen. Bekend geworden toepassingen uit de Eerste Wereldoorlog zijn de pestuitbraak in Sint Petersburg, de pakezels die in Mesopotanië waren geïnfecteerd met kwade droes en de pogingen om de paarden van de Franse cavalerie met droes te besmetten.

De wereld realiseerde de verschrikkingen van biologische en chemische

wapens en kwam op 17 juni 1925 tot het Protocol van Genève, dat inzet verbod. Er kwam echter geen controlerende instantie en de afspraak had daardoor weinig effect.

In de Tweede Wereldoorlog ontwikkelden diverse landen weer chemische en biologische wapens. De Japanners hadden een geheime biologische wapenfabriek in Manchoerije en voerden experimenten op Chinese krijgsgevangenen uit. Meer dan driehonderd gevangenen werden blootgesteld aan pest, miltvuur, syfilis en andere ziekten. De Japanners en de

*Clostridium botulinum*. Het is de meest toxische stof die de natuur produceert. Bij een besmetting met slechts één miljoenste van een milligram (0,001 microgram) sterft vijftig procent van de getroffenen. In vaktermen heet dit de LD50 (lethale dosis voor vijftig procent van de besmette groep).

De twee stoffen waren tot 1944 in gebruiksklare vorm opgeslagen om het toe te passen als de Duitse troepen biologische wapens zouden inzetten. De Britten ontwikkelden anthrax-

tuigen en in de ondergrondse de *Bacillus globigii* of de *Serratia marcescens* vrij.

In 1957 stopte de Britse overheid haar biologische wapenprogramma en vernietigde al haar voorraden. In 1969 stopten de Amerikanen hun ontwikkelingen van micro-organismen en in 1970 het onderzoek naar toxinen als aanvalswapen. In 1972 waren de Verenigde Staten een van de initiatiefnemers van de *Biological and Toxin Weapons Convention*. Ondanks het feit dat 162 landen (stand mei 2000) de op 26 maart 1975 opgestelde conventie te Moskou, Washington of Londen hebben ondertekend, is volgens generaal der mariniers Randall West, adviseur voor biologische wapens van de Amerikaanse minister van Defensie, het verdrag al minimaal tien maal geschonden. De verdragsschendende landen hebben anthrax als gebruiksklaar wapen of zijn actief bezig dit te ontwikkelen.



**Slachtoffer van inzet chemische wapens tijdens Iran-Irak-oorlog**

(Bron: abc-press)

Amerikanen werkten tevens aan de *Francisella tularensis*, een robuuste niet spore vormende bacterie, die wekenlang bij lage temperaturen kan overleven in water, modder, hooi en lijken, om het voor oorlogsvoering te kunnen gebruiken.

De Amerikanen openden in 1942 een *War Research Service*, dat anthraxsporen en de veroorzaker van botulisme ontwikkelde tot wapens. Het toxine dat botulisme veroorzaakt komt van de zuurstofminnende sporen vormende gram-positieve bacterie

bommen en testten deze gedurende de jaren 1942 en 1943 op het eiland Gruinard ten noordwesten van Schotland. De proefdieren (schapen) stierven snel en het eiland was daarna 45 jaar verboden gebied vanwege het besmettingsgevaar.

Ook na de Tweede Wereldoorlog vervolgden de Amerikanen hun onderzoek naar biologische wapens en lieten in de jaren vijftig en zestig wolken van onschadelijke bacteriën vrij op burgers, om de effecten van biologische wapens gericht tegen mensen te kunnen meten. Zij lieten vanuit vlieg-

Het voormalige hoofd van het biologische wapenprogramma van de Sovjet-Unie, Ken Alibek, bekend in zijn in 1998 uitgekomen boek *Biohazard*, dat de Russen zelfs tot in 1990 bezig waren met het geschikt maken van het pokkenvirus voor hun biologische bewapening. De activiteiten vonden plaats in een aantal instituten, die bekend waren onder de naam Biopreparat. De organisatie was in 1973 opgericht en had op een gegeven moment 25.000 mensen in dienst in twintig onderzoek-, ontwikkeling- en productiecentra. In 1979 vond een ongeval plaats in de wapenfabriek in Sverdlovsk waarbij 66 mensen stierven door inhalatie van vrijgekomen anthraxsporen. Niet alleen direct na het vrijkomen van de sporen, maar ook geruime tijd daarna, stierven omwonenden aan miltvuur. Hoewel het anthraxongeval goed was gedocumenteerd, gaven de Russische autoriteiten pas in 1992 het ongeluk toe. De biologische wapenfaciliteiten bevonden zich in de Oekraïne, Kazachstan en Oezbekistan. Deze instituten bestaan niet meer, maar het is onduidelijk waar de ontwikkelde kennis en producten zijn gebleven.

## Terroristen

De vrees bestaat dat terroristische organisaties en een aantal landen zoals Irak, Noord-Korea en Libië beschikken over de kennis en materialen om biologische wapens te construeren. In zijn 272 pagina dikke rapport *Chemical and Biological Defense Program* van maart 2000, verwachtte de Amerikaanse minister van Defensie de komende tien jaar een forse toename in de dreiging van biologische wapens door terroristen. De dreiging krijgt nog meer reliëf door het rapport *Advances in Biotechnology and Genetic Engineering: Implications for the Development of New Biological Warfare Agents*, dat het Pentagon in juni 1996 publiceerde. Hierin staat hoe eenvoudig men ziekteverwekkers kan veranderen, zodat ze levensbedreigend worden en moeilijker zijn te bestrijden. Micro-organismen evolueren sneller dan de mens en zijn buitengewoon inventief om hun erfelijke materiaal zo effectief mogelijk te gebruiken. Zo kan de *Staphylococcus aureus*, die normaal op de huid leeft en waarvan we nauwelijks iets merken, veranderen in de

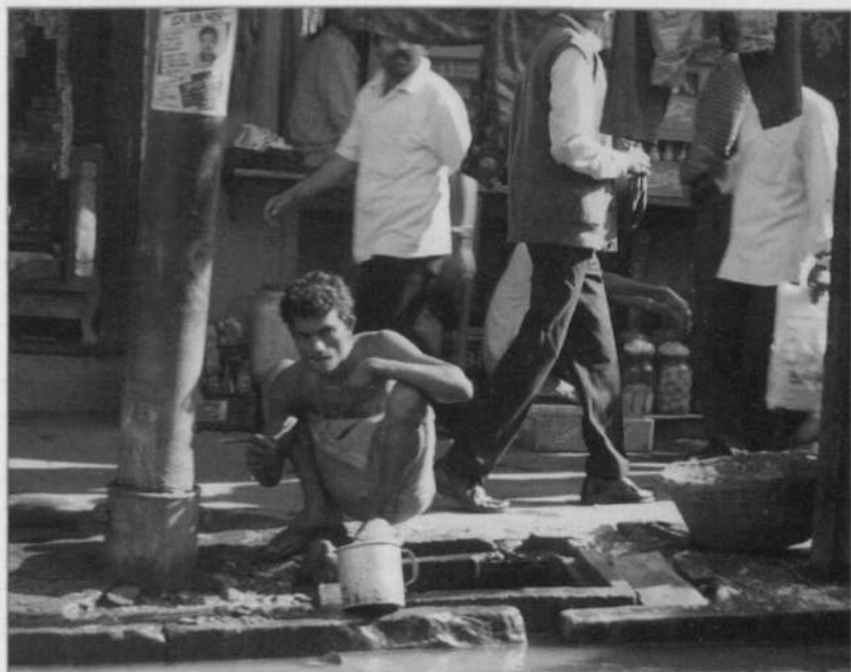
levensgevaarlijke MRSA (multi-resistente *Staphylococcus aureus*) bacterie. De bacterie heeft dan een ongevoeligheid voor de antibiotica, waarmee artsen normaal een bacteriële infectie bestrijden. Ook kan de bacterie stofjes maken, die actieve componenten van het niet-specifieke humane afweersysteem plat leggen, waardoor de bacterie ten koste van zijn gastheer kan overleven. Andere strategieën van bacteriën zijn het inkapselen, zoals de tuberculosebaciil doet om zich te onttrekken aan het menselijke afweersysteem, of het in de aanvallende cel gaan nestelen. Dat laatste doet de legionellabacterie. Men kan zich voorstellen dat als deze eigenschappen worden gecombineerd met andere eigenschappen van ziekmakende bacteriën, er een buitengewoon lethaal micro-organisme kan ontstaan. Ook met virussen kan men buitengewoon ziekmakende of snel lethale combinaties samenstellen met biotechnologische technieken. De natuur zal zo'n extreem virulente (ziekmakende) bacterie of virus niet zo snel maken, omdat de gastheer te snel sterft en het micro-organisme zich daardoor niet snel genoeg kan

vermenigvuldigen. Daardoor blijven ebola-epidemieën, waarbij de patiënten snel sterven, altijd regionaal beperkt.

Instituten die dergelijke virussen verzamelen, hebben de warme belangstelling van sommige landen of groeperingen. Ook onderzoekers, zoals recent de Australiërs Ron Jackson en Ian Ramshaw, die met biotechnologische technieken toevallig een zeer dodelijk pokkenvirus hebben geconstrueerd, kunnen hun laboratorium beter goed beveiligen. De terroristische bio-dreiging is ongeveer aan het begin van de jaren tachtig begonnen. Een van de eerste voorbeelden was de bewuste besmetting van saladebuffetten met *Salmonella typhimurium* in restaurants in Oregon (USA) door de volgelingen van Bhagwan Shree Rajneesh.

Het in maart 2000 verschenen rapport van de Amerikaanse defensieorganisatie noemt de landen Noord-Korea, China, India, Pakistan, Iran, Irak, Syrië en Libië als plaatsen waar nog steeds biologische wapens worden ontwikkeld en/of geproduceerd. Van deze landen zouden terroristen biologische wapens kunnen betrekken, of in die landen de benodigde grondstoffen of kennis kunnen vinden. Het is overigens niet bijzonder moeilijk om een biologisch wapenarsenaal in te richten.

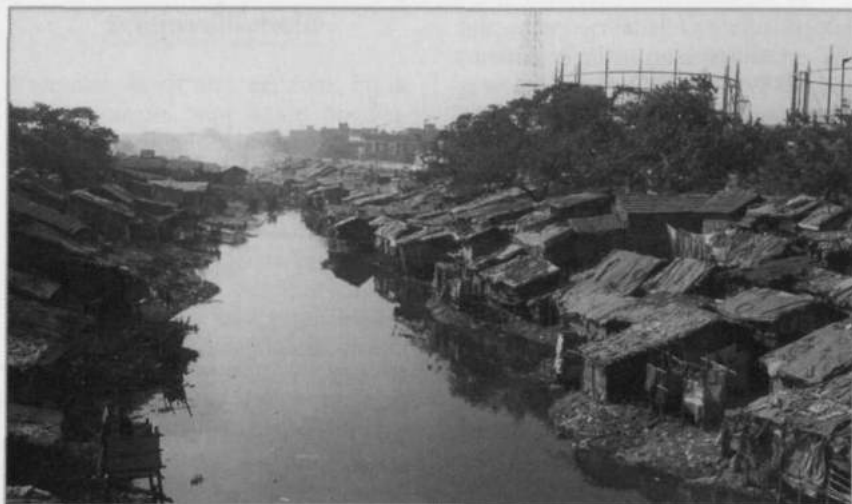
De ontrafelaar van het menselijke genoom, Graig Venter, van het Amerikaanse bedrijf Celera Genomics, denkt dat een organisme met slechts driehonderd genen kan leven. In de komende tien jaar zou zijn bedrijf zo'n basaal levend organisme kunnen maken en dit zou commercieel een succes kunnen worden. Biotechnologische bedrijven zouden met dit organisme medicijnen kunnen produceren. Venter stopte echter het project, toen duidelijk werd dat bioterroristische groepen het zouden kunnen gebruiken als superwapen. Toch zal het basale leven vroeg of laat geproduceerd worden, want de wetenschappelijke kennis om dit te doen is al aanwezig.



Vanwege zijn door de jaren getrainde afweersysteem, kan deze man in Calcutta zijn tanden poetsen met sterk vervuild water

## Penicilline resistente miltvuur

Tijdens Amerikaanse militair medische conferenties is anthrax, miltvuur, het meest genoemde biologische wapen. Het is bekend dat Noord-Korea beschikt over wapensystemen gevuld met penicilline resistente anthraxsporen, die in korte tijd grote populaties levensbedreigend ziek kunnen maken. Het grote gevaar van dit wapen is, dat bij ziekteverschijnselen de gebruikelijke behandeling met antibiotica niet werkzaam is. Anthrax is een buitengewoon effectief wapen voor de terrorist. Om een gebied van 100 km<sup>2</sup> zodanig te besmetten dat vijftig procent van de bevolking sterft, is acht ton van het uiterst giftige ricine nodig. Een kilo anthraxsporen heeft hetzelfde desastreuze resultaat. Bij inademing van tienduizend tot twintigduizend sporen van de *Bacillus anthracis*, de miltvuurbacterie, kan het slachtoffer al binnen een paar dagen sterven. Bij het ongeluk in Sverdlovsk bleken sommige in de nabijheid wonende mensen pas na zes weken de ziekteverschijnselen te krijgen. Volgens dr. Marc Kortepeter, officier preventieve genees-



Een culture van bacteriën uit deze beek (een wijk in Calcutta) in een waterleidingssysteem, kunnen een epidemie in de westerse wereld veroorzaken

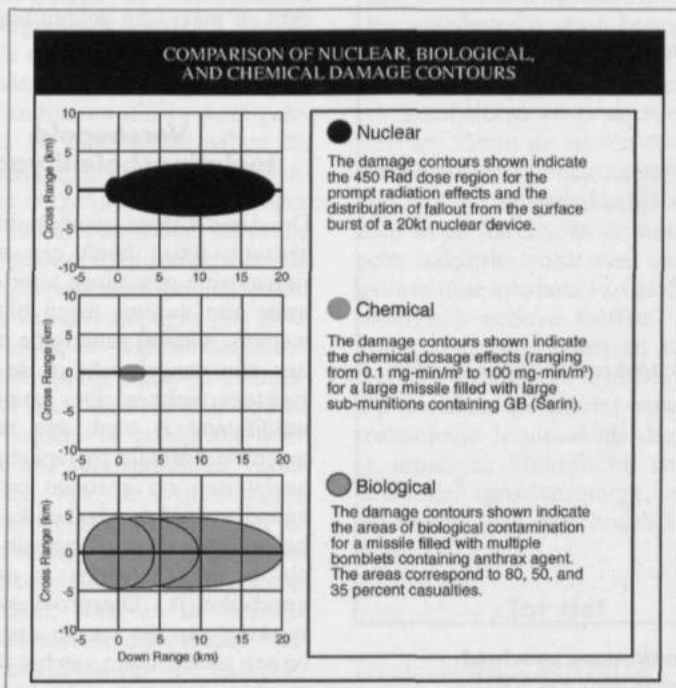
kunde bij de *Operational Medicine Division* van het USAMRIID, vormen de sporen in de bodem van een besmet gebied nog langdurig een gevaar voor de bevolking.

### Samenwerking met biotechnologische industrie

De Amerikaanse overheid heeft een groot aantal organisaties opdracht

gegeven een rol te vervullen binnen het *Biological Defense Program*. Vier ministeries, te weten defensie, volksgezondheid, landbouw en justitie zijn bij de voorbereidingen om bioterrorisme te bestrijden betrokken. Bij de ontwikkeling van nieuwe technieken speelt het DARPA *Biological Warfare Defense Program* (DARPA = *Defense Advanced Research Projects Agency*) een centrale rol. Dr. Michael Goldblatt van DARPA/BSO (*Defense Science Office*) is projectdirecteur voor de niet-conventionele verdediging tegen ziekteverwekkers. Zijn afdeling met twintig medewerkers besteedde vorig jaar 300 miljoen dollar aan research.

Er is veel geld beschikbaar voor onderzoek naar vaccins die effectief werken tegen de bekende biologische wapens. Het Californische biotech bedrijf Maxygen kreeg in september 1999 een bedrag van 6,7 miljoen dollar voor de ontwikkeling van inhalerbare vaccins. Zij kreeg dit bedrag van DARPA, bovenop een subsidie van 7,7 miljoen dollar in april 1999, voor de ontwikkeling van nieuwe vaccins gericht tegen antigenen, waarvoor nog geen vaccins zijn ontwikkeld. Met haar gepatenteerde *Molecular-Breeding™* techniek, in jargon ook bekend als *DNA Shuffling*, kan het in 1997 opgerichte Maxygen, door mid-



### Categorie A

Hoge prioriteit vanwege gemakkelijke verspreiding, besmetting, hoge mortaliteit en vanwege het geven van problemen bij de gezondheidszorg vanwege de behandeling.

- *Variola major* (pokken)
- *Bacillus anthracis* (anthrax)
- *Yersinia pestis* (pest)
- *Clostridium botulinum* toxine (botulisme)
- *Francisella tularensis* (tularemie)
- Filovirussen
- Ebola (hemorragische koorts = bloedingen of stolsels gevende koorts)
- Marburg ziekte (hemorragische koorts = bloedingen of stolsels gevende koorts)
- Arenavirussen
- Lassakoorts
- Junin (Argentijnse hemorragische koorts) en gerelateerde virussen

### Categorie B

Tweede prioriteit zijn agentia, die minder gemakkelijk zijn te verspreiden, een lagere morbiditeit hebben en specifieke kennis vereisen om de ziekte te herkennen.

- *Coxiella burnetti* (Q fever)
- *Brucella* soorten (micrococcus)
- *Burkholderia mallei* (kwade droes)
- Alphavirussen
- *Venezuelan equine encephalitis*
- *Eastern- en western equine encephalitis*
- Ricine toxine van *Ricinus communis* (castor bonen)
- Epsilon toxine van *Clostridium perfringens*
- *Staphylococcus enterotoxine B*

Een onderdeel van lijst B agentia zijn pathogenen, die in voedsel of water kunnen voorkomen.

- *Salmonella*
- *Shigella dysenteriae*
- *Escherichia coli* )157:H7
- *Vibrio cholerae* (cholera)
- *Cryptosporidium parvum*

### Categorie C

De derde categorie betreft agentia die pas in de toekomst zouden kunnen worden geproduceerd voor massavernietiging.

- Nipah virus
- Hantavirussen
- Hemorragische koortsvirussen in teken
- Encephalitis virussen in teken
- Gele koorts
- Multiresistente tuberculose

#### Potentiële biowapens volgens de Amerikaanse overheid

(Bron: Department of Health and Human Services (hhs), mei 2001)

del van genetische manipulatie, relatief gemakkelijk vaccins ontwikkelen voor nieuwe pathogenen, oftewel biologische wapens.

Het zijn de kleine innovatieve biotechbedrijven, die bij het onderzoek naar nieuwe vaccins zijn betrokken. Het Pentagon heeft via haar *Joint Vaccine Acquisition Programme* (JVAP) vorig jaar 322 miljoen dollar aan onderzoek besteed. Niet alleen Amerikaanse bedrijven profiteren hiervan, maar ook bijvoorbeeld het Franse bedrijf *Porton International* en het Britse *Centre for Applied Microbiology*, een *spin off* van het Britse bio-defensieprogramma, delen mee. Zover bekend zijn geen Nederlandse bedrijven of instituten betrokken bij het Amerikaanse onderzoek, hoewel het Prins Mauritslaboratorium van TNO actief is in het ontwikkelen van biosensoren voor de detectie van B-wapens. De grote farmaceutische bedrijven ontbreken in dit netwerk, omdat zij de te behalen winsten uit de defensieprojecten te laag vinden. De te verwachten opbrengsten uit militaire opdrachten zouden volgens een woordvoerder van de gevestigde farmaceutische industrie in geen verhouding staan met de marges van 65 procent en meer, die gelden binnen zijn bedrijf.

#### Versoepeld toelatingsbeleid vaccins

De Amerikaanse geneesmiddelenregistratie (FDA) heeft een uitzonderingspositie geschapen voor de registratie van vaccins tegen biologische wapens, waarbij genetische modificaties zijn aangebracht in de normale ziekteverwekker. De aangebrachte modificatie is vaak een resistentie tegen de normale therapieën. Veiligheidstesten op gezonde proefpersonen zijn altijd noodzakelijk, maar het bewijs voor de werking van het vaccin in proefpersonen is niet altijd noodzakelijk. Dierproeven om de werking van het vaccin aan te tonen en een goede uitleg van het werkingsmechanisme, zijn voldoende om de

FDA te overtuigen. Onder deze regeling vallen onder andere de botuline toxine-varianten. Het zijn stoffen die onmiddellijk doden en daarom door terroristen gebruikt zouden kunnen worden. Met een fatale dosis van 0,6 nanogram gif per kilogram lichaamsgewicht is botulisme toxine vele malen dodelijker dan zenuwgas.

### Het anthrax vaccinatieprogramma

Op 18 mei 1998 besloot de Amerikaanse regering een anthrax-vaccinatieprogramma uit te voeren, waarbij in 2006 alle Amerikaanse militairen en het burgerpersoneel van het Pentagon gevaccineerd moeten zijn. Volgens plan moeten vanaf 2003 jaarlijks 2,6 miljoen vaccinaties worden uitgevoerd. De vaccinatie omvat zes injecties in een periode van achttien maanden, gevolgd door een jaarlijkse booster. Het gebruikte vaccin komt van het Amerikaanse biotech bedrijf BioPort. Het in mei 1998 opgerichte bedrijf kocht de rechten van het anthraxvaccin van de *State of Michigan's Department of Public Health* (MDPH).

Niemand binnen de Amerikaanse defensieorganisatie kan zich aan de vaccinatie onttrekken. Een weigering is strafbaar. Het programma is begonnen met militairen die in Azië gelegerd zijn. De autoriteiten willen dat de militairen hun verplichte anthraxvaccinatie vergelijken met het dragen van een helm, een stukje uitrusting voor de persoonlijke veiligheid. Bij het defensiepersoneel bestaat vanaf het begin van de campagne een grote weerzin tegen de anthraxvaccinatie, hoewel het vaccin tegen de anthraxbacterie al sinds 1970 door de FDA als officieel vaccin is goedgekeurd en voor elke arts verkrijgbaar is. Vooral reservisten van de Amerikaanse luchtmacht hebben bedenkingen en laten hun collega's via internet weten hoe zij erover denken. Het Golfoorlogsyndroom, waarvan de oorzaak nog steeds niet is achterhaald, versterkt de afwijzing van alle bijzondere vaccinaties.

### Schijnveiligheid

Vaccinatie hoeft niet, net zoals bij de griepvaccinatie, een totale bescherming te bieden en daarom was de Amerikaanse *Defence Intelligence Agency* (DIA) zeer ongerust toen zij in 1997 in een medisch vakblad lasen, dat de Russische onderzoeker Andrey Pomerantsev een gemodificeerde vorm van anthrax had gemaakt. Dit gaf aanleiding tot het geheime project onder de codenaam *Project Jefferson*, dat een monster moest zien te bemachtigen van de gemodificeerde bacterie. Daar Amerika één van de ondertekenaars is van de *Biological Weapons Convention* van 1972, moest het werk omzichtig gebeuren om de gemaakte afspraken niet te schenden. Pentagon-woordvoester Victoria Clarke, kon op 4 september 2001 bekend maken dat DIA over de bacterie beschikte en na een nog te volgen juridische procedure, wetenschappelijk onderzoek aan de gemodificeerde anthrax kan laten doen.

Een andere kritiek op het Amerikaanse vaccinatiebeleid is de weg van infectie. Immers, het vaccin is destijds ontwikkeld voor schapenscheerders, die via hun handen konden worden geïnfecteerd door besmettelijke schapen. Bij een biologisch wapen, gebaseerd op anthrax, worden de sporen geïnhaleerd en is de besmetting directer. Zitten de sporen op dragers van ongeveer vijf micrometer grootte, dan worden ze gemakkelijk opgenomen in de longen. In de farmaceutische industrie wordt veel onderzoek gedaan naar inhalatie van deeltjes met biologisch actieve stoffen. Binnenkort komen twee bedrijven met inhaalbare insuline om injecties overbodig te maken. De daarbij ontwikkelde technologie is ideaal als drager van te inhaleren biologische strijdmiddelen. Een sproei-vliegtuigje, eventueel onbemand, kan het dodelijke werk doen.

### Tot slot

De geschiedenis leert dat de menselijke geest, ook als het gaat om perfidi-

teit, uiterst creatief kan zijn. Bioterrorisme verdient onze aandacht. Wie gewetenloos handelt kan met een biologisch wapen vele slachtoffers maken. Het instrument is minuscuul; de gevolgen kunnen desastreus zijn.

### Literatuur

- [http://www.house.gov/reform/ns/web\\_resources/briefing\\_memo\\_july\\_23.htm](http://www.house.gov/reform/ns/web_resources/briefing_memo_july_23.htm)  
Johns Hopkins Center for Civilian Biodefense Studies, <http://www.hopkins-biodefense.org>  
Clinton W.J., Remarks by the President on keeping America secure for the 21st Century, National Academy of Sciences, Washington DC, 22 januari, 1999.  
Shalala D.E., Bioterrorism: How prepared are we?; *Emerging Infectious Diseases*, 5(4), juli-augustus 1999.  
Rhein R., The first line in biodefense; *Scrip Magazine*, december 1999, p. 29.  
Stienstra S., Amerika bereidt zich voor op de dreiging van bio-terroristen, *Nederl. Milit. Geneesk. T.* 53, 83-86 (2000).  
Friedlander A.M. et al., Anthrax Vaccine: Evidence for safety and efficacy against inhalation anthrax; *JAMA*, Vol. 282 No. 22, 8 december 1999.  
Inglesby T.V. et al., Anthrax as a biological weapon: Medical and public health management; *JAMA*, 281: 1735-1745 (1999).  
Simon J., Biological Terrorism Preparing to meet the treat; *JAMA*, 278: 428-430 (1997).  
Stienstra S., HP komt als eerste met een commerciële 'Lab-on-a-chip analyser'; *Lab-briefing*, 9:12 (1999).  
US-DOD publication, Chemical and Biological Defense Program; Annual Report to Congress, maart 2000.  
Stienstra S., Amerika bereidt zich voor om bioterroristen voor te zijn. *Marineblad*, juni 2000.  
Albert M.R. et al., The last smallpox epidemic in Boston and the vaccination controversy, 1901-1903, *New England Journal of Medicine*. 344(5):375-9 (2001).  
Dennis C., The bugs of war. *Nature*. 411(6835):232-235 (2001).  
Fee E. et al., Preemptive Biopreparedness: Can We Learn Anything From History? *American Journal of Public Health*. 91(5):721-726 (2001).



# Information Operations: informatie als doel, middel én wapen

## Dreiging en kwetsbaarheden verbonden aan een bijzondere vorm van militair optreden

drs. J.A. van der Louw – luitenant-kolonel der fuseliers\*

### Inleiding

Sinds april 2001 kent de Nederlandse krijgsmacht beleid op het gebied van *Information Operations* (Info Ops). De minister van Defensie stemde toen in met het 'Beleidskader *Information Operations*', dat was opgesteld door een werkgroep onder leiding van de Defensiestaf (DS). In deze 'Werkgroep *Information Operations* Defensie' (WG IOD) waren vertegenwoordigd de krijgsmachtdelen, onderdelen van de Centrale Organisatie<sup>1</sup> en TNO. Het beleidskader gaat onder meer in op de risico's verbonden aan Info Ops, de rol van de mens, relevante nationale en internationale (met name NAVO-) ontwikkelingen en de juridische aspecten. Tevens worden aanbevelingen gedaan voor vervolgactiviteiten op het gebied van Info Ops en er wordt een ambitieniveau voor de Nederlandse krijgsmacht gepresenteerd.

\* De auteur is voorzitter van de Werkgroep *Information Operations* Defensie (WG IOD) en is werkzaam binnen de Defensiestaf/Stafafdeling Conceptuele Zaken. De auteur dankt ir. H.A.M. Luijck en dr. M.H.A. Klaver van TNO-FEL voor hun constructieve commentaar op een eerdere versie.

<sup>1</sup> Van de CO waren vertegenwoordigd in de WG IOD de Militaire Inlichtingendienst (MID), de Beveiligingsautoriteit (BA, deze ressorteert onder de secretaris-generaal), Defensiestaf/Nationale Plannen, Defensiestaf/CIS (inmiddels IV-'pool' genoemd) en de Directie Organisatie & Informatie (DOI) van de DGE&F.

In dit artikel wordt een tipje van de 'informatiesluier' opgelicht en ingegaan op enkele aspecten van deze vorm van (militair) optreden. Met name beschouwt dit artikel de dreiging van en door offensieve Info Ops, onze kwetsbaarheden op dit gebied en wat wij – als organisatie én als functionaris – daartegen kunnen doen. Allereerst wordt echter de actualiteit van het onderwerp verklaard en vindt een begripsbepaling plaats. Tevens wordt ingegaan op de koppeling met het functiegebied 'inlichtingen', het centrale thema van dit nummer van de *Militaire Spectator*.

### Info Ops: een actueel onderwerp

'De vijfde dimensie van het militaire spectrum [naast land, zee, lucht en ruimte]...'. 'Shaping the hearts and the minds...'. 'In peacekeeping operations, the word is our primary weapon system...'. 'To shape the perception of reality...'. 'De beslisser en de besluitvormingsprocessen als doel en informatie als wapen...'. 'Een alternatief manoeuvreermiddel...'. Al deze zinsneden hebben een relatie tot Info Ops. Ze roepen echter ook veel vragen op. Gaat het nu over elektronische oorlogvoering? Of juist over informatie in de zin van informatieverstrekking en *Public Information*? Welke relatie hebben psychologische operaties tot Info Ops? En hoe zit het eigenlijk met computeroorlogvoering? Naast

de noodzaak deze vragen te beantwoorden, is er een aantal redenen waarom een nationaal defensiebeleid op het gebied van Info Ops vereist was en eind 1999 een werkgroep daartoe aan het werk ging: activiteiten binnen de NAVO, de praktijk tijdens vredesoperaties, de afhankelijkheid van Defensie van informatie en de uitvoering van wetenschappelijk onderzoek naar Info Ops.

### De NAVO-dimensie

De NAVO houdt zich sinds enkele jaren actief bezig met de beleidsontwikkeling over Info Ops. Zo heeft de NAVO haar Info Ops-beleid vastgelegd in het Militaire Comité document 422 (MC 422), dat in januari 1999 door de Noord-Atlantische Raad (NAR) werd goedgekeurd. Het MC belastte tevens een werkgroep, de *NATO Information Operations Working Group* (NIOWG) met de verdere beleidsontwikkeling – in het bijzonder de actualisering van MC 422 – alsmede met de ontwikkeling van Info Ops-doctrine en het integreren van *lessons learned* in beleid en doctrine. Onder meer op basis van de ervaringen in Bosnië (IFOR, SFOR) en Kosovo (*Allied Force*, KFOR) zijn voorstellen gedaan aan het MC voor een aangepaste MC 422 en wordt gewerkt aan de *Allied Joint Publication* (AJP) 3.10 – Info Ops. Dit NAVO-beleid vormt een belangrijke bouwsteen voor het Nederlandse defensiebeleid: de consequenties



**Info Ops, een krachtig instrument bij vredesoperaties**

ervan en de vervolgactiviteiten voor de nationale 'spelers' moeten worden vastgesteld.

Info Ops vormen reeds enige jaren een integraal deel van militaire operaties, zoals bij IFOR/SFOR en KFOR (waarbij overigens de naamgeving 'Info Ops' tot voor kort ontbrak). Naar verwachting zal haar rol bij toekomstige militaire operaties alleen nog maar toenemen. Info Ops hebben immers in de praktijk bewezen een krachtig en (veelal) niet-letaal instrument bij vredesoperaties te zijn. Willen Nederlandse eenheden en stafpersoneel een adequate bijdrage kunnen leveren aan een militaire operatie in NAVO- of een ander coalitieverband, dan moet kennis van en inzicht in Info Ops zijn opgebouwd. Nationaal beleid is daarbij onmisbaar.

### **De nationale dimensie**

Defensie is in haar functioneren in toenemende mate afhankelijk van en wordt geconfronteerd met allerlei

vormen van informatie en informatievoorziening. Daarbij moet worden gedacht aan (geautomatiseerde) informatiesystemen, van Defensie zelf, van coalitiepartners en van systemen uit het publieke domein, maar ook aan publieke informatievoorziening door de media (bijvoorbeeld CNN). Als (logisch) gevolg daarvan nemen dreigingen en risico's toe. Om deze adequaat te kunnen pareren, moet Defensie beschikken over een adequate bescherming en reactiemogelijkheden in het geval van een 'aanval'. Met de verdere ontwikkeling van de kennis van en het inzicht in de offensieve mogelijkheden van Info Ops, ontstaat meer inzicht in de risico's en kunnen relevante beschermingsmaatregelen worden genomen. Op de militaire aspecten hiervan ga ik later in dit artikel nader in; de civiele kant ervan wordt uitgebreid belicht in het artikel van ir. Luijff.

Ten slotte voert het onderzoeksinstituut TNO (met name het Fysisch- en Elektronisch Laboratorium - FEL en Technische Menskunde - TM) in

opdracht van Defensie al enige jaren onderzoek uit op het gebied van Info Ops. Zo is TNO-FEL actief betrokken bij onderzoek naar de kwaliteit van de bescherming van de defensie-ICT-infrastructuur en onderzoekt TNO-TM de effectiviteit van PsyOps-boodschappen op de besluitvorming door commandanten.

Om de onderzoeksvragen door Defensie gericht te kunnen vaststellen en eventueel bij te sturen moet defensiebeleid zijn ontwikkeld waarin de grondslagen en ambities met betrekking tot Info Ops zijn vastgelegd.

De actualiteit van het onderwerp wordt bovendien onderstreept door de betrokkenheid van het ministerie van Defensie bij het nationale onderzoeksproject 'Infodrome'. Daarin wordt samen met andere ministeries gestudeerd op het overheidsbeleid voor de komende decennia ten aanzien van het gebruik van ICT in de zogeheten 'informatiesamenleving'. Daarbij komt ook de beleidsvraag aan de orde of (en op welke wijze) de staatsveiligheid in het geding kan zijn bij de verstoring van de nationale (essentiële) informatie-infrastructuur en die van de ons omringende landen. Heeft de overheid (en dus ook Defensie) een rol in de bescherming van inmiddels geprivatiseerde informatie-infrastructuren van bijvoorbeeld elektriciteitsmaatschappijen en telecommunicatiebedrijven, zeker indien de economie en de staatsveiligheid van Nederland in het geding zijn? Voor Defensie is deze discussie bovendien van belang omdat zij gebruik maakt van civiele infrastructuren bij de uitvoering van vredesoperaties en oefeningen. Ik verwijs verder graag naar het artikel van ir. Luijff.

### **Begripsbepaling**

De NAVO heeft met betrekking tot Info Ops een brede en complexe benadering gekozen. Info Ops richten zich in de NAVO-visie op het beïnvloeden van beslissers en besluitvormingsprocessen en is daarbij toepasbaar op poli-

tiëk-strategisch, militair-operationeel en tactisch niveau. De huidige versie van MC 422 stelt:

*The scope of Info Ops is extremely wide. (...) Info Ops affect all areas, civil and military, within all NATO headquarters and across strategic, operational and tactical boundaries and can be applied throughout the spectrum of conflict.*

De NAVO heeft met Info Ops ook een hoog ambitieniveau voor ogen. Info Ops kunnen een belangrijke bijdrage leveren aan het bereiken van de doelen van de NAVO, het voorkomen van potentiële crises, het reduceren van de lengte van een politieke of militaire confrontatie én het voorkomen van het gebruik van militair geweld.

Info Ops vormen ook een middel om te komen tot een betere integratie van het politieke consultatieproces, het besluitvormingsproces en de militaire operaties van de Alliantie. Het centrale thema daarbij is 'coördinatie', de afstemming van de inzet van de verschillende 'aandachtsgebieden'. Het doel van Info Ops is door de NAVO zeer ruim geformuleerd: van informatie via besluitvormingsprocessen naar fysieke systemen. De term *Information Operations* benadrukt daarbij de overheersende rol van informatie als doel, als middel én als wapen. Het is echter onjuist om bij 'informatie' alleen te denken aan digitale vormen van informatie. Info Ops zijn dan ook niet voorbehouden aan het gebruik van 'hightech'-middelen. Ook het uitdelen van pamfletten in het kader van psychologische operaties en het bouwen van een Bailey-brug, kunnen namelijk bijdragen aan het bereiken van de gestelde Info Ops-doelstellingen.

Het recent goedgekeurde beleidskader presenteert een Nederlandse definitie van het begrip *Information Operations*, waarbij is uitgegaan van de NAVO-definitie uit MC 422,<sup>2</sup> aangevuld met en aangepast aan enkele specifiek nationale inzichten. De Nederlandse definitie luidt:

*Information Operations (Info Ops) zijn activiteiten gericht op het beïnvloeden van beslissers ter ondersteuning van politieke en militaire doelstellingen door de informatie, besluitvormingsprocessen, commandovoeringsmiddelen en ondersteunende communicatie en informatiesystemen van een opponent aan te grijpen en gelijktijdig de eigen informatie, processen en systemen te benutten en te beschermen. Er zijn twee vormen van Info Ops: defensieve en offensieve Info Ops, afhankelijk van de aard van de betreffende activiteiten.*

Info Ops kennen nadrukkelijk géén eigen capaciteiten (hooguit enige stafcapaciteit), maar betreffen uitsluitend de coördinatie van de capaciteiten van andere beleidsterreinen. Deze worden in het Nederlandse beleidskader aangeduid met de term 'aandachtsgebieden', waarbij onderscheid wordt gemaakt tussen de niet-militaire en militaire aandachtsgebieden. De eerste zijn politieke activiteiten, diplomatieke activiteiten, civiel-militaire samenwerking (CIMIC), *Public Information* (de Britten spreken in dit verband van 'Media Ops') en de informatie-infrastructuur. De militaire aandachtsgebieden vormen tezamen *Command and Control Warfare* (C2W) en betreffen fysieke vernietiging, elektronische oorlogvoering (EOV), misleiding, psychologische operaties (PsyOps) en operationele veiligheid. Deze militaire aandachtsgebieden – en dit geldt ook voor sommige niet-militaire aandachtsgebieden – worden ondersteund door het

<sup>2</sup> De NAVO-definitie van Info Ops luidt: Actions taken to influence decision-makers in support of political and military objectives by affecting other's information, information based processes, command and control capabilities and supporting communication and information systems while exploiting and protecting one's own. There are two categories of Info Ops: defensive Info Ops and offensive Info Ops, depending upon the nature of the actions involved.

inlichtingenproces (*All Source Intelligence*) en communicatie- en informatiesystemen (CIS). Er is dus géén sprake van de inbedding van bijvoorbeeld *Public Information*, CIMIC of C2W in Info Ops, wel dragen deze aandachtsgebieden – mits zij voor wat betreft de uitvoering op elkaar afgestemd zijn – bij tot het bereiken van de Info Ops-doelstellingen.

### **Een nadere verklaring van de Nederlandse definitie**

Allereerst de term 'benutten' (NAVO: *exploiting*). Hieronder verstaan wij het optimale gebruik van informatie die in de organisatie aanwezig is en die verborgen blijft, tenzij aandacht wordt geschonken aan het mogelijke belang van die informatie voor anderen. Informatiestromen kunnen worden geïntegreerd ter verhoging van de *situational awareness* van verschillende eenheden (*joint* en multinationaal) binnen hetzelfde operatiegebied en van de beslissers op de verschillende niveaus van militaire commandovoering en de politiek. Informatie moet snel, tijdig en integer op de juiste plaats beschikbaar komen. ICT biedt in toenemende mate mogelijkheden dit te realiseren, al zijn er ook nadelen aan verbonden. Door een grotere interoperabiliteit van communicatiesystemen nemen de informatiestromen namelijk sterk toe. Informatie-filtering, *overload*-bescherming en vooral aandacht voor de mens als beslissers, moeten dan ook de nodige aandacht krijgen om de beschikbare informatie beheersbaar (en bruikbaar) te houden.

Er zijn twee vormen van Info Ops: defensieve en offensieve Info Ops. Bij *defensieve Info Ops* gaat het om het voorkomen van beïnvloeding door een opponent of partij in een conflict. (Zie schema op blz. 631) *Offensieve Info Ops* zijn het spiegelbeeld van het bovenstaande en gericht op de zwakke punten op de genoemde gebieden bij een opponent.

- de actieve en passieve bescherming van militaire eenheden, de politieke en militaire beslissers en de eigen samenleving tegen psychologische operaties en misleiding;
- het voorkomen van ongewenste beïnvloeding van eigen beslissers en besluitvormingsprocessen door woord, geschrift, beeldmateriaal, televisie- of radio-uitzendingen of andere vormen van communicatie;
- het zo mogelijk voorkomen van de aantasting – en indien nodig herstellen – van de exclusiviteit (de vertrouwelijkheid), integriteit (de betrouwbaarheid) en beschikbaarheid van informatie en geautomatiseerde informatiesystemen (het 'beschermen van de elektronische flank');
- het inschatten van de capaciteiten en potentiële aanvalsmethoden van een opponent die offensieve Info Ops kan uitvoeren of uitvoert.

### Het domein Info Ops

Ten slotte nog aandacht voor het volgende. De term Info Ops benadrukt de centrale rol van informatie: als doel, als middel én als wapen. Een van de doelstellingen van Info Ops is het verkrijgen van een informatievoorsprong in termen van tijd, kwantiteit en vooral kwaliteit: eerder en beter zijn geïnformeerd dan de opponent. De Verenigde Staten spreken in dit verband van *information dominance*. Die informatievoorsprong moet dan worden omgezet in samenhangende acties die de opponent de wil en het vermogen ontnemen om zich verder te verzetten of zelf effectieve acties te ondernemen. Informatie kan zich daarbij in verschillende verschijningsvormen presenteren: het gesproken of geschreven woord, geschrift, beeldmateriaal, televisie- of radio-uitzendingen of communicatie

in digitale vorm. Het is dus bepaald onjuist om bij informatie alleen maar, of vooral, te denken aan digitale vormen van informatie of aan (nog specifiek) Internet. Het is evenzeer onjuist om Info Ops synoniem te stellen met computeroorlogvoering. Hoewel het een wezenlijke component ervan is, ligt de kracht van het NAVO- en Nederlandse Info Ops-concept immers juist in de brede benadering: door de afstemming van bijvoorbeeld CIMIC-activiteiten, PsyOps, *Public Information* en computeroorlogvoering wordt de effectiviteit van die – op zichzelf staande – activiteiten versterkt.

In het Nederlandse Beleidskader *Information Operations* is een eenvoudig schematisch model opgenomen (zie blz. 632) waarin de belangrijkste componenten van Info Ops in samenhang met elkaar worden gepresenteerd: de politieke en militaire doelstellingen die worden nagestreefd met de betreffende operatie, de militaire en niet-militaire aandachtsgebieden die tezamen leiden tot het bereiken van de vastgestelde doelstellingen, de daarbij te hanteren werkwijze (coördinatie en harmonisatie van alle inspanningen) en het uiteindelijke doel van de Info Ops: het beïnvloeden van de beslissers van de opponent of partijen.

### Inlichtingen

#### Het fundament

Het belang van accurate, tijdige en volledige inlichtingen over potentiële tegenstanders en hun mogelijkheden, intenties en gebruik van (offensieve) Info Ops is evident. Het Nederlandse model voor Info Ops onderstreept nog eens de fundamentele plaats van inlichtingen hierbij. Deze komt duidelijk naar voren in de *Command and Control Warfare*-'tempel', waar *All Source Intelligence* het fundament vormt voor CIS en de vijf 'pilaren' van C2w. Overigens geldt de noodzaak van adequate inlichtingen ook voor de meeste van de niet-militaire aandachtsgebieden. Het is immers ondenkbaar dat diplomaten hun werk

kunnen doen zonder over achtergrondinformatie te beschikken over de personen en partijen met wie zij onderhandelen. Ook de planning van CIMIC-activiteiten staat en valt met goede inlichtingen over de situatie in het operatiegebied.

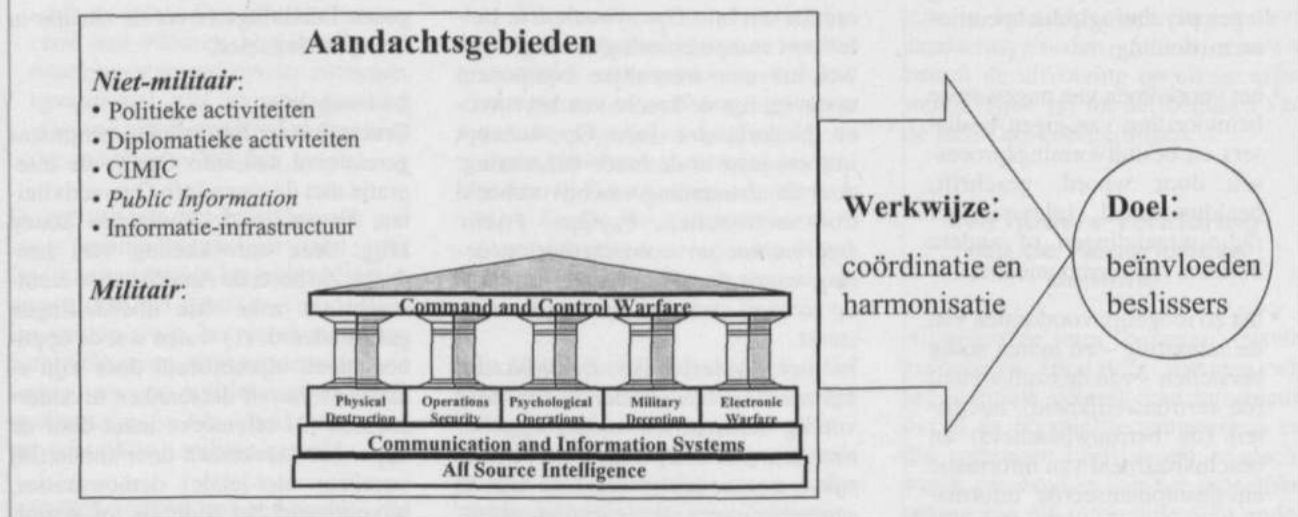
#### De integratie

Cruciaal voor het inlichtingenproces gerelateerd aan Info Ops is de integratie met de eigen Info Ops-activiteiten. Vooral in de Verenigde Staten krijgt deze ontwikkeling veel aandacht. Zo heeft de Amerikaanse luchtmacht ter zake drie doelstellingen geformuleerd: (1) weten wat de opponent doet, bijvoorbeeld door zijn e-mail te lezen of databanken te onderzoeken; (2) offensieve inzet door de opponent voorkomen door snelle (bij voorkeur niet-letale) demonstraties, bijvoorbeeld het tijdelijk (of definitief) uitschakelen van de elektriciteitsvoorziening of het manipuleren van televisie-uitzendingen; (3) lokaliseren van commandovoerings- en verbindingsknooppunten en andere *high value targets* (zoals mobiele luchtverdediging en ballistische raketten) en deze met een minimum aan bijkomende schade en verliezen aan mensenlevens uitschakelen. Deze benadering is weliswaar specifiek toegesneden op de Amerikaanse situatie, maar op hoofdlijnen ook toepasbaar in de Nederlandse context. Of Nederland eventueel de beschikbare Info Ops-capaciteiten offensief zal inzetten, hangt naast de politieke besluitvorming bovenal af van een goede inschatting van de dreiging, de mogelijkheden een 'aanval' te voorkomen en een adequate identificatie van mogelijke 'doelen'. Bovendien dient inzicht te bestaan in de reactie van een opponent: is de inschatting dat de beslisser wordt beïnvloed door onze actie, of wordt hij of zij juist 'eigenwijzer'.

### De dreiging

Een groot aantal landen (*states of concern*) beschikt over offensieve Info Ops-capaciteiten. Zo zijn er lan-

## Information Operations



### Het Nederlandse model van Info Ops

den waarbij psychologische operaties een integraal deel vormen van het optreden van de overheid, de inlichtingen- en veiligheidsdiensten en het militaire apparaat. In sommige landen maken offensieve 'cyberoperaties' (het gebruik van onder meer computers voor militaire doeleinden) reeds deel uit van de militaire doctrine en zijn ook het EOv-beleid en -doctrine ver ontwikkeld, volledig geïntegreerd in de gevechtsvoering en in belangrijke mate offensief georiënteerd. In weer andere landen zijn mediamanipulatie en censuur van staatswege prominent aanwezig. De vraag is wel in hoeverre deze landen ook de intentie hebben hun offensieve Info Ops-capaciteiten daadwerkelijk te gebruiken tegen de NAVO (-lidstaten) en meer specifiek Nederland en de Nederlandse defensieorganisatie.

Uit 'open' bronnen valt enorm veel informatie te verkrijgen over de mogelijkheden, intenties en toepassingen van landen op het gebied van bijvoorbeeld computeroorlogvoering. Bladen als *Jane's Defence Weekly* en *Defense News* doen regelmatig verslag van de recente ontwikkelingen. In Nederland hebben onder meer

*NRC/Handelsblad, Vrij Nederland* en *HP/De Tijd* in 1999 en 2000 in algemene zin aandacht besteed aan dit thema. Ter illustratie van het voorgaande een voorbeeld: China. De *US Congressional Research Service* (een onafhankelijk onderzoeksbureau van de *Library of Congress*) heeft in november 2000 een rapport uitgegeven waarin de activiteiten van China op het gebied van cyberoperaties worden beschreven. Een citaat uit dit rapport:

*'China is developing a strategic information warfare unit to neutralize the military capabilities of technologically advanced foes. The unit, dubbed Net Force, will wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems'.*

Volgens andere bronnen beschikt China inmiddels over zo'n 1000 zogenoemde 'Cybersoldaten' en maken Info Ops inmiddels deel uit van de trainingen van militaire staven. Naast China beschikken nog zo'n 30 (!) andere landen over militaire 'hacker'-teams.

Naast de groep 'landen' is er een aantal andere actoren dat zich met aspecten van Info Ops (in het bijzonder het gebruik van computers, informatie en geautomatiseerde informatiesystemen) bezighoudt. Voorbeelden hiervan zijn terroristische groeperingen, actiegroepen, de georganiseerde misdaad en bepaalde individuen.

#### Terroristische groeperingen

Er is weliswaar geen groepering die op dit moment wordt onderkend als een direct risico voor de Nederlandse defensiebelangen, maar als NAVO-lid mag Nederland deze dreiging niet veronachtzamen. Terroristische organisaties richten zich doorgaans vooral op prestigieuze doelen en naar verwachting zal een terroristische dreiging zich dan ook waarschijnlijk vooral concentreren op de grotere NAVO-landen. Echter, ook beslissers, besluitvormingsprocessen en geautomatiseerde informatiesystemen van kleinere landen zoals Nederland, kunnen een aantrekkelijk doelwit van offensieve Info Ops vormen.

#### Actiegroepen

Ook met bepaalde actiegroepen moet steeds meer rekening worden gehou-

den. Zij maken vooral gebruik van moderne communicatie- en informatietechnologie om snel gegevens uit te wisselen, hun achterban te mobiliseren en voor het breed uitdragen van hun doelstellingen. Welke groep op welk moment een zeker risico vormt, hangt met name af van de operaties waaraan Nederland deelneemt of van plan is dat te doen. Het is ook denkbaar dat bij Nederlands militair optreden in het buitenland, vertegenwoordigers van betrokken bevolkingsgroepen trachten de Nederlandse militaire of civiele beslissers of besluitvormingsprocessen 'aan te vallen' (lees: te beïnvloeden).

#### Georganiseerde misdaad

De georganiseerde misdaad zal zich vooral concentreren op financiële winst (hetgeen zich 'vertaalt' in het gebruik van financiële transactiesystemen, financieel berichtenverkeer en logistiek verkeer) en de verkoop van ongeautoriseerd verkregen (militaire)

informatie. Deze doelgroep kan echter ook belang hebben bij het verstoren of destabiliseren van een (vrede)soperatie, meer in het bijzonder van bijvoorbeeld de CIMIC-activiteiten daarbinnen.

#### Individueen

Sommige individuen (denk aan hackers) hebben grote belangstelling voor systemen van de overheid, in het bijzonder die van defensieorganisaties. De beweegredenen zijn zeer divers: uitdaging, ideële overwegingen, ontvreemden van informatie, aanbrengen van mutaties, gebruik van diensten. Met geringe eigen middelen kan men aan de slag en veel meer dan een goede personal computer en een modem zijn niet nodig. De dreiging ligt daarbij niet zozeer bij de individuele hacker, maar vooral bij diegenen die hun expertise in dienst stellen van derden, bijvoorbeeld van *states of concern* of aan een terroristische groepering.

## Kwetsbaarheden

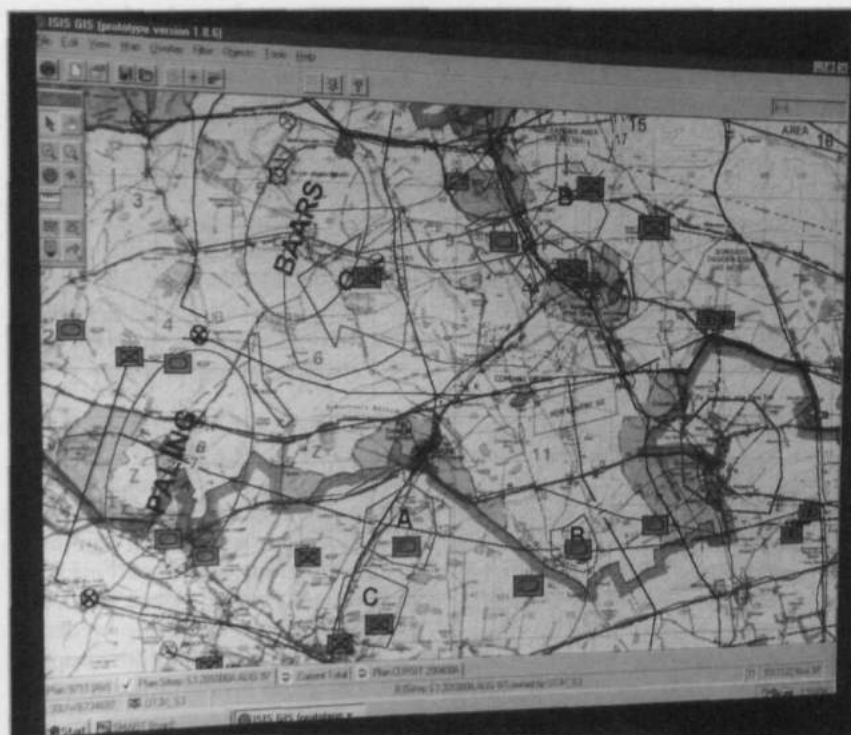
De kwetsbaarheid van Defensie voor offensieve Info Ops neemt toe. De oorzaken zijn velerlei. De belangrijkste zijn: de afhankelijkheid van informatie, het gebruik van civiele technologieën, de introductie van nieuwe technologieën, de proliferatie van netwerken, de afhankelijkheid van bondgenoten, het veiligheidsbewustzijn van het eigen personeel en adequate reactiemechanismen.

#### Afhankelijkheid van informatie

Informatie en ICT spelen een steeds grotere rol in de samenleving. Ook beslissers binnen Defensie zijn in toenemende mate afhankelijk van informatie en geautomatiseerde informatiesystemen, zowel tijdens het operationeel optreden als bij de vredesbedrijfsvoering. Zo is het tijdens operaties van groot belang steeds over een actueel en volledig inzicht in de situatie te beschikken. Het is voor com-



Internet: een nieuwe werkelijkheid



### Afhankelijkheid van informatie

mandanten op elk niveau cruciaal om te beschikken over zowel een totaalbeeld als over de mogelijkheid om 'in te zoomen' op een lokale situatie met mogelijk politiek-strategische betekenis. Het moderne militaire optreden wordt daarnaast gekenmerkt door een grote behoefte aan informatie-uitwisseling met bondgenoten, niet-gouvernementele organisaties en andere departementen. Ook in het kader van de logistieke ondersteuning tijdens operaties wordt steeds vaker gebruik gemaakt van civiele informatie-infrastructuren. Kortom, de betrouwbaarheid van informatie en geautomatiseerde informatiesystemen en de integriteit van informatie-infrastructuren, vormen in toenemende mate een kritieke factor voor het succes van de operatie en daarmee een potentieel aangrijpingspunt voor een opponent.

#### Gebruik civiele technologieën

De gebruikte systemen en technologieën zijn steeds vaker gebaseerd op civiele standaarden. De snelle ontwikkelingen op het gebied van informatie en ICT noodzaken steeds vaker

tot het verwerven van *Commercial-off-the-shelf* (COTS) middelen en diensten. Adequate technische beveiligingsmiddelen zijn duur, moeilijk te implementeren en veelal nog niet beschikbaar. Verder kennen opposenten de gebruikte programmatuur vaak ook, inbegrepen de 'achterdeuren' ervan. Ook is er sprake van een toenemende verstrengeling van militaire informatiestructuren met die van civiele organisaties. Zo worden voor militaire communicatie steeds vaker civiele netwerken gebruikt. Daarbij worden grotere gevoeligheden voor verstoringen door natuurlijke oorzaken, technische storingen en onopzettelijke menselijke fouten voor lief genomen.

#### Introductie nieuwe technologieën

De snelle ontwikkelingen op het gebied van informatie en ICT leiden ertoe dat er steeds meer en steeds sneller nieuwe producten en diensten op de markt verschijnen. Defensie is – als iedere andere (overheids)organisatie – kwetsbaar voor de vaak snelle

en uit beveiligingsoogpunt niet altijd doordachte introductie van nieuwe technologieën. Het gevaar bestaat dat bij de aanschaf van nieuwe technologieën de beveiligings- en beheersaspecten te weinig aandacht krijgen.

#### Proliferatie van netwerken

Om de informatie-uitwisseling te versnellen en te verbeteren worden computers steeds vaker aan elkaar gekoppeld in netwerken. Deze netwerken worden vervolgens veelal onderling verbonden. In het algemeen geldt dat met de grootte van het netwerk en het aantal gebruikers (ook telewerkers!) ook de kwetsbaarheid toeneemt. Is iemand eenmaal binnengedrongen in een deel van het defensienetwerk, dan is het voor hem of haar relatief eenvoudig ook andere delen ervan binnen te gaan en daar gegevens te kopiëren, te vernietigen of (ongemerkt) te wijzigen.

#### Afhankelijkheid van bondgenoten

Nederland neemt in beginsel in NAVO- of ander coalitieverband deel aan vredesoperaties. Daardoor kunnen dreigingen en risico's die initieel gericht zijn op de coalitiepartners ook effect hebben op de Nederlandse defensie. Nederlandse besluitvormingsprocessen en geautomatiseerde informatiesystemen zijn immers veelal geïntegreerd in die van de NAVO of coalitie. In toenemende mate wordt de Nederlandse defensie daarmee afhankelijk van middelen die niet onder haar controle staan.

#### Veiligheidsbewustzijn van het personeel

Informatie (ook gerubriceerde) kan relatief eenvoudig ongeautoriseerd worden verspreid binnen de organisatie als ook naar buiten en binnen toe (bijvoorbeeld via e-mail). Daarbij vormt extern ingehuurd personeel een extra risicofactor. In het algemeen geldt dat het beveiligingsbewustzijn en de kennis van beveiligingsmaatregelen van het personeel niet altijd op het gewenste niveau zijn. Niet alle defensiemedewerkers zijn zich er voldoende van bewust dat informatie ook

een wapen kan zijn dat tegen (de leden van) de eigen organisatie kan worden gebruikt.

#### Adequate reactiemechanismen

Defensie beschikt nog niet overal over goed toegeruste mechanismen waarmee mogelijke inbreuken op de informatiebeveiliging kunnen worden onderkend en onderzocht. Ook een snelle en adequate reactie op onderkende gevaren is nog niet in alle gevallen mogelijk.

### Maatregelen

Het Beleidskader Info Ops presenteert een groot aantal maatregelen op het gebied van Info Ops. Daarbij worden vier categorieën onderscheiden: defensieve, offensieve en ondersteunende maatregelen, alsmede maatregelen op het gebied van training en opleiding. Het voert te ver om in dit artikel op alle maatregelen in te gaan, derhalve worden slechts enkele ervan hierna genoemd, ter illustratie van de denkrichtingen. Zo wordt een *Information Operations Coördinatie Cel* (tocc) ingesteld binnen de Defensiestaf. Dit is een (niet-permanent aanwezig) organisatie-element dat de verantwoordelijkheid draagt voor de

coördinatie van alle Info Ops-activiteiten tijdens de planning en uitvoering van vredes- en artikel 5-operaties. Voorts worden gerichte *inlichtingenactiviteiten* uitgevoerd, erop gericht de capaciteiten, intenties en activiteiten van potentiële tegenpartijen vast te stellen.

#### Verbeteren van de bescherming

Een andere maatregel betreft het verbeteren van de bescherming van de geautomatiseerde informatiesystemen, netwerken en procedures. Daartoe worden zogeheten afhankelijkheids- en kwetsbaarheidsanalyses (A&K-analyse) uitgevoerd die de kwetsbaarheden kunnen vaststellen. Daarbij wordt gebruik gemaakt van de zogenoemde *red teams* en *green teams*, die (heimelijk respectievelijk openlijk) de kwetsbaarheden blootleggen door (te proberen) binnen te dringen in de defensienetwerken en -systemen. Vervolgens worden de geconstateerde knelpunten vermindert of opgelost door het nemen van concrete beveiligingsmaatregelen.

#### Technologische ondersteuning

Ook het gebruik van technologische ondersteuning ten behoeve van de besluitvorming moet worden genoemd als 'verbetermaatregel'. Zo kunnen

*Decision Support Systems* commandanten helpen de beschikbare informatie te analyseren en op basis daarvan beslissingen te nemen. Een deel van het onderzoek van TNO is hierop gericht. Ten slotte dienen Info Ops te worden geïntegreerd in *training en opleiding*. Op de KMA gebeurt dit reeds, maar dit verdient navolging bij andere opleidingsinstituten. Zo dienen Info Ops tijdens oefeningen op alle niveaus een centrale(re) rol te krijgen, zoals de NAVO doet bij haar CJTF HQ-trials.

### Tot slot

De vraag rijst wat Defensie verder kan doen om de dreiging en de kwetsbaarheden verbonden aan Info Ops het hoofd te bieden. Alles staat en valt daarbij met het 'bewustzijn' bij het personeel van de (potentiële) dreiging die uitgaat van offensieve Info Ops-activiteiten – in de vredeslocatie en tijdens (vredes)operaties – en van de geconstateerde kwetsbaarheden. Artikelen zoals deze en het uitdragen van de Nederlandse beleidsvisie met betrekking tot Info Ops, dragen er hopelijk aan bij dat het defensiepersoneel zich hiervan meer bewust wordt.



# Bitbreuken verwacht; zijn wij erop voorbereid?

## Onze kwetsbare informatie-infrastructuren

ir. H.A.M. Luijff\*

### Inleiding

Onze samenleving verandert snel door het razendsnelle tempo van elkaar inhalende informatie- en communicatietechnologie (ICT) ontwikkelingen. Nieuwe toepassingen, de convergentie van elektronische diensten en een wereldomspannende verwevenheid van complexe informatie-infrastructuren zorgen er voor dat er met name in de Westerse wereld sprake is van een sterk opkomende 'informatiemaatschappij'. Onder *informatie-infrastructuren* verstaan we het geheel aan apparatuur, programmatuur en verbindingen om informatie tussen één persoon (of een voor hem/haar werkend programma) en een netwerkdienst (welke op zich een keten van diensten kan zijn) uit te wisselen.

Er is de afgelopen jaren een toenevende bezorgdheid bij inlichtingendiensten en overheden in verschillende, vooral westerse, landen ontstaan over de kwetsbaarheid van de informatie-infrastructuren die gebruikt worden door onze krijgsmachten, overheden en samenlevingen. Alle zegeningen van ICT ten spijt kunnen informatie-infrastructuren echter gelijk-

tijdig de Achilleshiel van de samenleving en/of defensie zijn. Er is een toenemende dreiging van asymmetrisch optreden door zowel reguliere als ook irreguliere tegenstanders en hun supporters, waarbij onze ICT het doelwit is. Daarbij vallen termen als Info-warriors, Cyber-terroristen en (h)activisten.

Ook onze Nederlandse informatie-infrastructuren kunnen een aantrekkelijk doelwit zijn. In verschillende studies wordt onderkend dat schade als gevolg van Cyber-activisme of computeroorlogvoering aan Nederlandse civiele en militaire informatie-infrastructuren zowel een strategische als operationele impact kan hebben op Nederlandse militaire operaties in NAVO- of ander coalitieverband. Is onze samenleving überhaupt voorbereid op grootschalige storingen, laat staan moedwillig veroorzaakte verstoringen, in onze ICT-infrastructuren? En wie moet er dan wat doen?

In dit artikel behandel ik de brede problematiek van kwetsbare informatie-infrastructuren en geef ik aan wat onze Nederlandse overheid en Defensie hier inmiddels aan doen. Tot slot volgt de conclusie.

### Risicobeheersing of ogen en oren dicht?

Defensieorganisaties, zoals de Nederlandse, maken steeds meer gebruik van ICT. Daarbij wordt in toenemende mate gebruik gemaakt van *commercial-off-the-shelf* (COTS) producten

(bijvoorbeeld PC's, Windows/NT) en van publieke diensten, bijvoorbeeld de satellietverbinding via KPN-Burum met onze, aan de NAVO of de VN ter beschikking gestelde, Nederlandse eenheden in het buitenland.

Naast vele positieve ontwikkelingen ontstaan bij invoering van iedere nieuwe technologie ook risico's. De manifestatie daarvan lijkt voor de mens en de samenleving vaak stoetsgewijs plaats te vinden. Leereffecten van een cluster van incidenten met nieuwe technologie, denk bijvoorbeeld aan ontploffende stoomketels in de beginperiode van de industriële revolutie en aan de elektriciteitsongevallen eind negentiende en begin van de twintigste eeuw, hebben altijd geleid tot overheidsmaatregelen die de risico's voor mens en samenleving beheersbaar moeten maken. Ik noem als voorbeeld de wettelijke eisen aan stoomketels en de controle door het Stoomwezen. Dergelijke maatregelen hebben een dempend effect op de negatieve gevolgen van de invoering van nieuwe technologie. Dat gaat goed tot een nieuw probleem zich aanmeldt.

Parallel aan de explosieve en dynamische ICT-ontwikkeling is er de beweging van een terugtrekkende overheid en liberalisatie van infrastructuurdiensten, waarbij de 'markt' zelfregulerend de bescherming tegen de risico's van negatieve effecten op zich moet nemen. Iets dat vroeger een overheidstaak was, maar waar de overheid nu graag de andere kant uitkijkt.

\* De auteur is principal consultant bij het TNO Fysisch en Elektronisch Laboratorium. Hij verricht onderzoek op de gebieden Informatie Operaties, bescherming van kritische informatie-infrastructuren en informatiebeveiliging. Hij bedankt de reviewers mw. dr. M.H. A. Klaver en lkol. drs. J.A. van der Louw voor hun nuttige commentaren. Hij is gaarne bereid een literatuurlijst ter beschikking te stellen: luijff@fel.tno.nl



De slagaders van de moderne maatschappij (Bron: foto Nico Schouten)

De complexe, reeds vergaande en steeds sneller toenemende informatie- en communicatieafhankelijkheid en -verwevenheid van bedrijven, overheid en ook Defensie, maakt deze ongedacht kwetsbaar. Bij onderzoekers, Westerse inlichtingendiensten en vooral de Angelsaksische overheden, is in de afgelopen jaren een toenemende bezorgdheid ontstaan over de kwetsbaarheid van de informatie-infrastructuren.

Inmiddels uiten ook in Nederland multi-nationals, grote bedrijven, belangbehartigers – als de Verbond Nederlandse Ondernemingen-Nederlands Christelijk Werkgeversverbond (VNO-NCW) – en markt-actoren uit de ICT-sector, hun bezorgdheid over de kwetsbaarheid van onze informatie-infrastructuren. Waar is die bezorgdheid op gebaseerd?

### De relatie met Informatie Operaties (Info Ops)

Bij militaire operaties is het van oudsher belangrijk geweest om te onderkennen wat de zwakke plekken van

een tegenstander zijn. Reeds lang geleden tekende Sun Tzu daar verstandige dingen over op. De informatievoorziening voor *command & control* en de logistieke voorzieningen bleken vaak de zwakke plek te vormen. Ook heden ten dage zal men in een conflict proberen zijn sterke kant uit te buiten en de opponent ferm te raken in diens zwakke plek. Sommige westerse strijdkrachten streven ernaar om door informatie-operaties *information dominance* of zelfs *information superiority* te bereiken. Systemen en netwerken worden daarvoor aan elkaar gekoppeld en concepten als *Network Centric Warfare* doen opgang. Bij onvoldoende aandacht voor effectieve beschermende maatregelen creëren wij daarmee echter ook een Achilleshiel.

Het Beleidskader *Information Operations* en de daaraan voorafgaande Duits-Nederlandse stafstudie *Information Operations*, welke werd uitgevoerd door het *Amt für Studien und Übungen der Bundeswehr*, de afdeling Conceptuele Zaken van de Nederlandse Defensiestaf, de KMA en

TNO, beschrijven beide asymmetrische dreigingen door zowel reguliere als irreguliere opponenten. Het ultieme doel van *Information Operations*, de beïnvloeding van de tegenstander, kan niet alleen door militaire acties bereikt worden maar juist ook door beïnvloeding van de samenleving achter de militaire commandant of de politieke beslisser.

Ernstige versterking of zelfs de vernietiging van delen van civiele informatie-infrastructuren zijn daarbij een mogelijk drukmiddel van een opponent. De druk om (eigen) verliezen en *collateral damage* zo beperkt mogelijk te houden kan ertoe leiden dat computeroorlogvoering als onderdeel van offensieve Info Ops een zeer wel aanvaardbare, niet-letale militaire optie is. Het artikel van luitenant-kolonel drs. J.A. van der Louw, elders in dit nummer, geeft een uitgebreide behandeling van het Beleidskader Info Ops en de achterliggende concepten.

Overigens geldt hierbij hetzelfde internationale (oorlogs)recht als voor alle overige strijdmiddelen, zeker in het geval dat bij schade aan de informatie-infrastructuur lijfsgevaar voor non-combattanten ontstaat: bijvoorbeeld de uitval van informatiesystemen in ziekenhuizen. Of irreguliere tegenstanders of hun sympathisanten zoals (h)activisten en Cyber-terroristen vooraf zullen nadenken over de mogelijke consequenties gegeven het internationale recht, is maar de vraag. Hun doel bereiken vinden zij vermoedelijk belangrijker.

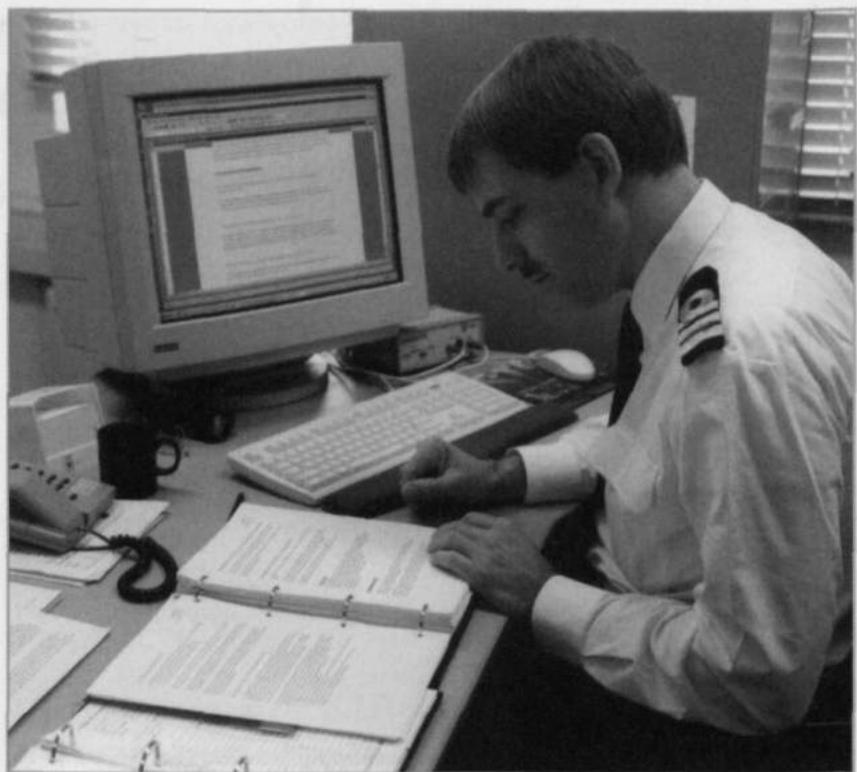
### Mogelijke militaire consequenties

Informatie-infrastructuurproblemen zijn niet voorbehouden aan civiele netwerken, maar kunnen ook in de operationele en de statische netwerken van Defensie voorkomen, ook al worden daar hogere beveiligingseisen aan gesteld. Defensie maakt ook gebruik van civiele informatie-infrastructuren. Daarnaast hebben ook de defensienetwerken de neiging om

snel complexer te worden met meer verweven en convergerende diensten, waarbij de beschikbaarheid van informatie een steeds belangrijker factor wordt. Een goede bescherming van de civiele ICT-infrastructuren en van de eigen defensie-infrastructuren is dus van groot belang voor Defensie. Zeker als daarbij rekening gehouden moet worden met asymmetrisch opererende tegenstanders en (h)activisme.

**Onderzoek naar de Nederlandse kwetsbare informatie-infrastructuren**  
De *Defensienota 2000* constateerde de toenemende ICT-kwetsbaarheid binnen en buiten Defensie, doch verbond daar op dat moment geen directe conclusies aan. Door Defensie is echter begin 2000, mede als gevolg van het nadenken over Info Ops-dreigingen en het millenniumprobleem, het onderwerp 'kwetsbaarheid van ICT' nadrukkelijk op de onderzoeksagenda van Infodrome geplaatst. Infodrome, onder leiding van staatssecretaris Rick van der Ploeg, is de denktank van het kabinet die tot taak heeft de consequenties voor het overheidsbeleid van het toenemend ICT-gebruik in de samenleving in kaart te brengen. Het door TNO in opdracht van Infodrome geschreven essay 'Bitbreuk' bekijkt de kwetsbaarheidsproblematiek vanuit het publieke domein en stelt een aantal hypothesen voor nader onderzoek. Aangehouden wordt dat 'bitbreuken' op allerlei niveaus kunnen optreden.

De individuele burger kan het vertrouwen in de elektronische overheid of het 'elektronisch winkelen' verliezen als het elektronische bancaire systeem hapert of uitvalt. Maar ook andere gebeurtenissen kunnen ernstige effecten hebben. Denk aan het uitvallen van onderliggende diensten zoals het Internet-domeinnaamsysteem; aan het haperen van koppelingen tussen diensten, zoals bij het telefoonverkeer tussen mobiel en het vaste net; aan haperingen in besturingsprogrammatuur, kabelbreuken en het uitvallen van stroomvoorzieningen.



#### Digitale krijgsmacht

(Bron: Centrum voor Audiovisuele Dienstverlening Koninklijke Marine, sectie fotografie)

In juni 2001 is door een groep experts van onder meer grote bedrijven en sectorverenigingen een manifest opgesteld met als titel 'Het kwict-instituut. Regulerend én stimulerend naar een betrouwbare ICT-infrastructuur'. Dit manifest is op 28 juni 2001 aangeboden aan overheid en politiek en behelst een voorstel tot publiek-private aanpak van de als urgent geziene ICT-kwetsbaarheid. Medio 2000 heeft het ministerie van Verkeer en Waterstaat aan Stratix/TNO de opdracht gegeven voor een studie naar de kwetsbaarheid van het Internet (KWINT). Het eindrapport KWINT stelt dat het (Nederlandse deel van) Internet kwetsbaar is en beveelt een aantal maatregelen aan om de kwetsbaarheid op korte en middellange termijn te verkleinen. De resultaten van deze studie zijn daarna door het ministerie van Verkeer en Waterstaat verwerkt in een beleidsnota voor het kabinet welke op 6 juli 2001 door de Ministerraad is aanvaard. De komende periode zal een aantal van

de voorgestelde maatregelen nader uitgewerkt worden.

#### Dubbele paradox

In de studie *Stroomloos* door het Rathenau-instituut naar de kwetsbaarheid van de stroomvoorziening wordt de zogenaamde *kwetsbaarheidsparadox* qua voorzieningen beschreven, waaraan ook de bovengenoemde Bitbreuk en KWINT studies refereren:

*Naarmate een land minder kwetsbaar is in haar voorzieningen, komt iedere verstoring van de productie, distributie en consumptie van die voorzieningen des te harder aan.*

Steetskamp en Van Wijk stellen zelfs dat er sprake is van een *dubbele paradox*:

*Als voorzieningen betrouwbaar lijken, gaan we ze in steeds sterkere mate gebruiken.*

Let wel, het gaat hierbij om de *menselijke perceptie* van betrouwbaarheid, niet om de technisch meetbare betrouwbaarheid. Voor ICT-infrastructuren geldt de genoemde dubbele paradox met name voor het beveiligingsaspect beschikbaarheid. De consequentie is dat alternatieve infrastructures, omdat ze minder gebruikt worden, vervolgens opgeheven worden. Een voorbeeld is de snelle verschuiving van betaalcheques naar pinpassen, waardoor banken besluiten de cheques uit te faseren. De consequenties kunnen groot zijn: uitval van het elektronisch pinnen kwam tot voor kort sporadisch voor. Als u op een zaterdagmiddag in de supermarkt eens een dergelijke uitval heeft meegemaakt, weet u welke paniek er dan uitbreekt bij een aanzienlijk deel van de klanten. Men heeft geen enkele rekening met een kans op storing gehouden. Men heeft geen stuiver kleingeld op zak. Landelijke uitval van pin-betalen op zaterdag 23 december 2000 had grote economische schade tot gevolg, maar had even zo goed tot openbare ordeproblemen kunnen leiden.

De hogere beschikbaarheid, integriteit en exclusiviteit van voorzieningen waarop ook uw informatievoorziening in haar vele verschijningsvormen is gebaseerd (bijvoorbeeld netwerkdienst, PC, mobiele telefoon, tv) leidt tot een zeer geringe tolerantie van mensen voor verstoringen in die voorzieningen. Defensie in haar relatie met bijvoorbeeld toeleveringsbedrijven, maar ook uzelf in het maken van afspraken en plannen gaan door de *perceptie* van een hoge betrouwbaarheid van ICT steeds strakker plannen, veel strakker dan gebaseerd op de leverantieafspraken, zoals bijvoorbeeld vastgelegd in *service level agreements*, verstandig zou zijn. En als het dan ook maar even fout gaat, blijken wij collectief vaak niet meer in staat om prioriteiten te stellen; om alternatieve communicatiemethoden te gebruiken en zijn de vroegere processen en procedures niet meer bekend.

### De complexe informatie-infrastructuur

Voor de Bitbreuk- en KWINT-studies zijn verschillende modellen ontwikkeld. Deze modellen zijn door Van Till en mij in detail beschreven. Met behulp van het ontwikkelde lagenmodel is de complexe kwetsbaarheid inzichtelijk gemaakt voor alle betrokkenen. Het fundament van dit lagenmodel wordt gevormd door de elektriciteitsvoorziening. Om te communi-

ceren hebben we een verbindingsweg nodig: de zogenaamde transmissie-laag, bijvoorbeeld telefoniekabels, glasvezel, 'de kabel' en zenders en ontvangers voor GSM. Ook deze transmissieapparatuur vergt elektriciteit. De netwerklaag heeft enige intelligentie waardoor informatie van de zender naar de bestemming geleid wordt: daarboven vinden een laag met een aantal basisdiensten. Denk aan diensten om elektronisch te betalen, databases die er voor zorgen dat bij-



Digitale maatschappij (Bron: Heerenveense Courant)

voorbeeld [www.mindef.nl](http://www.mindef.nl) vertaald wordt in een zogenaamd IP-adres of dat een telefoonnummer verwijst naar de locatie van zender(s) nabij een opgeroepen mobiele telefoon. Op dit stelsel bouwen eindgebruikers en bedrijven hun eigen toepassingen en kunnen tegenwoordig zelf ook als dienstenaanbieder, bijvoorbeeld als muziekdistributeur, in de publieke infrastructuur opereren.

### Facetten

De complexiteit van informatie-infrastructuren kent een aantal facetten. Ten eerste komt de civiele informatie-infrastructuur tot stand door het samenwerken van vele partijen die in één of meer van de hierboven lagen met hun dienstverlening actief zijn. Dit kan sterk lokaal gebonden zijn (de 'last mile' provider), regionaal (bijvoorbeeld Internet Service Provider), landelijk (bijvoorbeeld ISP of telecommunicatieaanbieder) en internationaal (bijvoorbeeld onderzeese kabels, satellietcommunicatie aanbieder).

Ten tweede is er – zoals eerder gesteld – een sterke convergentie gaande, waarbij diensten van de ene infrastructuur (in toenemende mate) door een andere infrastructuur geleverd worden. Daarbij wordt bijvoorbeeld gebruik gemaakt van zogenaamde gateways. Hierbij ontstaan (horizontale) ketens aan ICT-diensten waar informatie – onopgemerkt voor de eindgebruikers – verschillende bewerkingsstappen ondergaat. U hoeft niet te weten of uw collega op vakantie is in Tsjechië of Engeland, als uw e-mail maar op zijn mobiele telefoon terechtkomt. Of dat dan in de vorm van e-mail, een SMS-bericht of gesproken voice-mail is, maakt daarbij nauwelijks uit.

Ten derde de verwevenheid van diensten die gebruik maken van dezelfde netwerklaag en/of transmissiemiddelen. Denk bijvoorbeeld aan het gezamenlijk gebruik van NAFIN door Defensie, Binnenlandse Zaken en

Justitie, waarbij op de netwerklaag de LAN Interconnect (NafNet), het defensie-intranet, het General Purpose Voice Network (GVPN), het c2 Voice Network (C2VN), Ground-Air Voice Network (GAVN), videoconferencing, veiligheidszorginformatie (camerabewaking; alarmering; controle) en dergelijke lopen.

### Het effect

Al deze informatiestromen kunnen in één fysieke glasvezelbundel samenkomen, terwijl de eindgebruiker deze ICT-diensten als volkomen van elkaar gescheiden ervaart. De verwevenheid en convergentie blijkt als risico daardoor nogal eens over het hoofd gezien te worden, zowel bij het netwerkontwerp als bij het opstellen van calamiteitenplannen waarbij ICT als middel ingezet wordt: GSM bleek bij de Enschederamp als communicatiemedium door hulpdiensten gebruikt te worden. Is er dan sprake van meer samenvallende *single-point-of-failures* (SPOFs), dan kan een simpele storing als een kabelbreuk maar ook een gerichte *denial-of-service* aanval door een kwaadwillende leiden tot ernstige (ver)storingen met grote impact.

### Enkele incidenten

Defensieorganisaties, bedrijven en de Nederlandse samenleving worden regelmatig geconfronteerd met ernstige ICT-storingen en (pogingen tot) verstoringen. Ze worden vaak nog lacherig afgedaan als incidenten, de werkelijke risico's worden vaak niet onder ogen gezien. Het Melissa-virus in 1999 en de I-Love-You-worm die op 4 mei 2000 toesloeg waren nog onschuldige waarschuwingen. Wereldwijd bedreog de schade van I-Love-You drie miljard gulden, waarvan vijftig miljoen in Nederland. Ook vier ministeries waren het slachtoffer. Om De Wijk te citeren:

*Als dergelijke ontwrichtingen zich vaker gaan voordoen wordt het ver-*

*trouwen van de burger in ICT-netwerken ondermijnd.*

Enkele dagen na de uitbraak van het MKZ-virus liepen de gemoederen her en der hoog op en moest de ME ingezet worden omdat boeren vonden dat ze geen tijdige en adequate informatie kregen. Eén week voor de MKZ-uitbraak lag binnen het ministerie van Landbouw het gehele netwerk gedurende meer dan een dag plat ten gevolge van het Anna Kournikova-virus. Een geluk bij een ongeluk?

De Amerikaanse marine dacht begin 2001 dat een netwerkkapparaat (router) in hun operationele Intranet defect was. Men kreeg er geen bit meer doorheen en wilde de router al vervangen door een reserve-exemplaar. Een 'aanval' als oorzaak kwam niet in de geachte op. Toch was dit het resultaat van een zogenaamde *denial-of-service* (DOS) aanval. Veel later bleek dat de Australische Defensie ook slachtoffer was van dezelfde DOS-aanval. Niet alleen overheids-, ook civiele netwerken worden 'uit Cyberspace geblazen'.

Recent overkwam dat een informatie-beveiligingswebsite in Noorwegen. Deze kreeg een aanval van twee Gigabit/s gedurende meer dan vierentwintig uur te verwerken!

De Bitbreuk en KWINT-studies signaleren dat in Nederland gebieden zijn waar er gebrek aan voldoende elektriciteitsdistributiecapaciteit is ontstaan ten gevolge van de explosieve groei van ICT. Zo vergen zogenaamde data-hotels, locaties waar duizenden informatiesystemen staan die gekoppeld zijn aan een snelle glasvezelinfrastructuur, al gauw tussen de twintig en zestig MW, een stroomafname die overeen komt met die van een behoorlijke staalfabriek. Deze data-hotels staan dicht bij elkaar en zijn met name aan de zuidrand van Amsterdam te vinden. Door de explosieve groei in webservern en andere diensten loopt de aanleg van benodigde elektriciteitskabels fors achter op de behoefte en bestaande kabels wor-



### Blikseminslag is voldoende

(Bron: Heerenveense Courant)

den dan ook tot hun piekcapaciteit benut.

Zo ook op 5 juli 2001, een heel warme dag. Door de extra benodigde stroom voor de aircos werden stroomkabels te heet en werden automatisch afgeschakeld om een kabelsmelt te voorkomen. Daardoor viel op verschillende plaatsen in en rond Amsterdam de stroom uit. Ook het vitale knooppunt van het Nederlandse en Europese Internetverkeer, de Amsterdam Internet Exchange (AMS-IX), werd getroffen. Toen bleek dat veel apparatuur van de vele Internetdienstenaanbieders op dit cruciale verbindingsknooppunt voor de 24-uurs economie nog niet op een noodstroomvoorziening aangesloten was.

### Onderzoek in het buitenland

In de vs heeft de *President's Commission on Critical Infrastructure Protection* (PCCIP), met vertegenwoordigers van overheid, de informatie- en telecommunicatiesector, energiesector, financiële instellingen,

transport en vitale (hulp)dienstensector, in 1997, in haar eindverslag gesteld dat de complexe, veelal op ICT-gebaseerde infrastructures in de vs zeer kwetsbaar zijn voor een heel scala aan oorzaken, van ijzel tot aanslagen. De vs heeft vervolgens een aantal actieplannen in gang gezet, die eind 2003 concreet moeten leiden tot een sterk verminderde kwetsbaarheid.

Zwitserland heeft sinds 1997 vele zwakke plekken in de infrastructuur gedicht nadat ze er achter kwamen dat het gehele interbancaire netwerk bestuurd en gecontroleerd werd vanuit Dallas. In juni 2001 is de oefening *Informo* gehouden waarbij het federale ICT-crisisresponseteam, dat grootschalige verstoringen in de Zwitserse infrastructuur moet bestrijden, aan de tand gevoeld is.

Canada volgt een pragmatische werkwijze, waarbij optimaal gebruik is gemaakt van de inventarisaties tijdens de millenniumvoorbereiding. Het Canadese *Department of National Defense* (DND) heeft daarbij de coördinatie voor de gehele overheid gekregen en werkt daarbij nauw samen met hun 'Info Ops cell'.

Ook andere landen als Australië, Denemarken, Noorwegen, Zweden, Engeland, Duitsland en Japan hebben vergelijkbare studies naar de kwetsbare informatie-infrastructures uitgevoerd of zijn bezig met het treffen van beschermingsmaatregelen. De *KWINT*-studie beschrijft een groot aantal van die activiteiten en analyseert de sterke en zwakke punten. Duidelijk is dat competitie tussen verschillende overheidsorganisaties leidt tot verbrokkeling van de energie en tot ineffectieve aanpak van de problematiek. Noch de overheid, noch de marktpartijen kunnen het probleem in hun eentje aan. Een publiek-private samenwerking is dus vereist. Maar dat vergt wel een stevige vertrouwensbasis tussen alle partijen.

### Is Nederland voorbereid?

Zijn wij als Nederlandse samenleving überhaupt voorbereid op het bestrijden van een grootschalige uitval van onze ICT-infrastructures, hetzij door een grootschalige storing, hetzij door opzet? Het antwoord is nee. Tot op

heden is er nog geen instantie aangewezen die de coördinatie bij calamiteiten in onze ICT-infrastructuren ter hand moet nemen, de gevolgschade minimaliseert en zorgt dat er zo spoedig mogelijk weer sprake is van een beheersbare situatie. Nederland kent nog geen beleid zoals dat in de VS verwoord wordt in: *'outages from attack are rare, brief, limited geographically, manageable and minimally detrimental to the economy'*.

### Rampenplan

*Momenteel ontbreekt een rampenplan en is ook niet duidelijk welke organisaties coördinerend moeten optreden wanneer er iets mis gaat. Gezien de grote maatschappelijke impact die storingen in ICT-netwerken ten gevolge kunnen hebben vinden wij dat de overheid in dezen initiatieven moet gaan ontplooiën,*

constateerde De Wijk tijdens de Infodrome-presentatie over het KWICT-instituut.

Vooralsnog zijn in Nederland de volgende ministeries aan zet: Defensie voor de eigen infrastructuur, Binnenlandse Zaken voor openbare orde en veiligheid en inlichtingen, Binnenlandse Zaken/Grootstedenbeleid voor coördinatie van de ICT-ontwikkeling binnen de overheid, Economische Zaken in het kader van de ontwikkeling van de Digitale Delta en de beveiliging van de Nederlandse industrie, Verkeer en Waterstaat voor telecom-municatiediensten en infrastructuur,

Buitenlandse Zaken met betrekking tot internationale afstemming en Justitie voor computercriminaliteit.

KWINT constateerde dat door gebrek aan coördinatie kennis en middelen inefficiënt en ineffectief ingezet worden. Wel is inmiddels een aantal overheidsactiviteiten in gang gezet in het kader van de KWINT-nota. Zo is er een *'Computer Emergency Response Team'* voor de overheid in ontwikkeling bij Binnenlandse Zaken (CERT-BZK) welke mogelijk ook een (tijdelijke) rol krijgt als nationale CERT. De zogenaamde *'motie Wijn'* over kwetsbaarheid van de Nederlandse samenleving door het gebruik van ICT zal dit najaar waarschijnlijk resulteren in de instelling van een werkgroep/commissie. Die zal in korte tijd een actieplan moet ontwikkelen om de vitale voorzieningen van Nederland welke mede gebaseerd zijn op ICT – denk bijvoorbeeld aan de meet- en regelnetwerken van onze gasdistributie – minder kwetsbaar te maken. Hierbij wordt voortgebouwd op de KWINT-aanpak.

Nederland heeft ten opzichte van andere landen één groot voordeel maar tegelijk ook een nadeel: het poldermodel. We kunnen een dergelijke problematiek goed in alle gezamenlijkheid aanpakken, maar soms gaat consensus ten koste van slagvaardigheid. Gegeven de snelle ontwikkeling van de dreiging en de noodzaak om effectief te kunnen ingrijpen bij incidenten, is er snel capaciteit nodig om vierentwintig uur per dag en zeven dagen per week te reageren.

### Conclusie

Als we niet oppassen kan ICT een Trojaans Paard zijn; onze eigen kwetsbare Achilleshiel. Grote economische schade, een haperende samenleving en openbare orde en veiligheidsproblemen en een ineffectieve defensie kunnen de consequenties zijn van een grootschalige (ver)storing in onze informatie-infrastructuren. Voor een potentiële activist en (ir)reguliere tegenstander in een conflict een aantrekkelijke gedachte. Zeker omdat er grote effecten kunnen zijn tegen lage kosten, de middelen op de hoek te koop zijn en de kans op een succesvolle vervolging van computer-criminelen wereldwijd gezien laag is. Het is dus alleszins tijd om door meer managementaandacht te komen tot betere beveiliging van de informatie-infrastructuur, opleidingen waarin infrastructuur- en informatiebeveiliging ruimer aan bod komt, en een snelle reactiecapaciteit. Dit om de terpen waarop onze veelal verweven kritische civiele, civiel-militaire en militaire infrastructuren gefundeerd zijn, te verhogen en droog te houden. Maar bovenal moet er eerst sprake zijn van bewustwording van de risico's en de gezamenlijke verantwoordelijkheid om die beheersbaar te maken: In de woorden van Infodrome:

*Ook al heeft u de eigen stoep geveegd betekent dat niet dat de stad schoon is.*

Webverwijzing: [www.infodrome.nl](http://www.infodrome.nl)  
[www.tno.nl/instit/fel](http://www.tno.nl/instit/fel)

# De Russische diensten en hun verleden

drs. B.M. de Jong\*

De Russische president Boris Jeltsin ondertekende op 20 december 1995 een decreet van grote symbolische betekenis. Hij riep 20 december daarbij namelijk uit tot de 'Dag van de werker van de organen van staatsveiligheid van de Russische Federatie'. Dat er zo'n dag werd vastgesteld is op zich niet bijzonder. Net als in de voormalige Sovjet-Unie zijn er in het huidige Rusland speciale dagen voor tal van overheidswerknemers, zoals artsen, onderwijzers, politiemannen en leden van het korps grenstroepen.

Het belang van het werk van de betrokken overheidsdiensten wordt dan van verschillende zijden onderstreept, diensthoofden worden in de pers geïnterviewd en dergelijke. Dat personeel van de buitenlandse inlichtingendienst SVR, de federale veiligheidsdienst FSB, de afluisterdienst FAPSI en andere inlichtingen- en veiligheidsdiensten ook zo'n speciale dag kregen, is daarom niet ongewoon.

Pikant was echter wel de keuze van 20 december. Die datum was namelijk gekozen vanwege de oprichting van Lenins geheime politie Tsjeka (de Buitengewone Commissie ter Bestrijding van Contra-Revolutie en Sabotage) op 20 december 1917. Dat op dezelfde datum drie jaar later formeel de buitenlandse afdeling van de Tsjeka, de inlichtingendienst, werd opgericht, maakt 20 december dus ook tot een zeer geschikte feestdag voor de huidige SVR.<sup>1</sup>

President Jeltsin maakte met zijn daad duidelijk dat de huidige Russische overheid een duidelijke continuïteit ziet tussen de inlichtingen- en veiligheidsdiensten van de Sovjet-Unie en die van het huidige Rusland. Dat is vreemd als men bedenkt hoeveel slachtoffers de Tsjeka, de NKVD, de KGB en hoe die diensten verder geheven hebben, in en buiten de Sovjet-Unie hebben gemaakt. Het past ook binnen deze zienswijze dat president Jeltsin in juni 1994 diverse voormalige inlichtingsofficieren van de NKVD/KGB deels postuum onderscheidde. Hij deed dat vanwege het werk dat de betrokken inlichtingsofficieren voor de Sovjet-Unie hadden verricht, onder andere op het gebied van atoomspionage tijdens de Tweede Wereldoorlog. Hen werd de onderscheiding 'Held van Rusland' verleend.

In dit artikel behandel ik de manier waarop de huidige Russische inlichtingen- en veiligheidsdiensten met het verleden van hun voorgangers omgaan. Daartoe zal ik onder meer ingaan op publicaties die na 1991 bij

westerse uitgeverijen van de persen zijn gerold, waarvoor de Russische overheid materiaal uit de archieven van de eigen diensten beschikbaar heeft gesteld.

## PR-beleid onder Krjoetsjkov

Traditioneel werd het doen en laten van de KGB in de media en in publicaties in de Sovjet-Unie nauwelijks belicht. Een docent aan de Academie van de FSB typeerde onlangs de geheimhouding met betrekking tot de KGB in de jaren na Stalins dood in de Sovjet-Unie als volgt:

*Het publiek wist van het bestaan van geheime diensten, maar precieze informatie over de doelen, taken en werkwijze van de organen van staatsveiligheid kon men aan open bronnen niet ontlennen. Een sluier van geheimhouding lag over alles wat maar deed denken aan de KGB of ermee verbonden was. Sterker nog, er was in feite geen enkele wet- of regelgeving openbaar waaruit men iets te weten kon komen over welke sovjetorganen van staatsveiligheid er bestonden en wat hun structuur was.<sup>2</sup>*

Er verschenen in de Sovjet-Unie wel eens boeken en artikelen over iemand als Felix Dzerzjinski, het eerste hoofd van de Tsjeka onder Lenin, maar dergelijke publicaties waren geen serieuze historische werken. De onkritische teneur deed nog het meeste denken aan een hagiografie uit de tijd van het

\* De auteur is verbonden aan het Oost-Europa Instituut van de Universiteit van Amsterdam.

<sup>1</sup> De inlichtingen- en veiligheidsdienst van de Sovjet-Unie heeft in de loop der tijden vele namen gehad. Voor dit artikel is het van belang te weten dat de Tsjeka de benaming was voor de dienst in de eerste jaren onder Lenin. Tijdens de Stalinterreur was er in 1934-1946 sprake van de NKVD en de KGB heeft bestaan in de jaren 1954-1991.

<sup>2</sup> A.I. Pozjarov, 'KGB SSSR v 1950-1960-e gody: problemy istoriografii,' *Otetsjstvennaja istorija*, ('De KGB van de USSR in de jaren '50 en '60: historiografische problemen,' *Vaderlandse geschiedenis*,) mei-juni 2001, p. 141.



rijke Roomse leven. Aan de terughoudendheid in de sovjetmedia, ten aanzien van alles wat met staatsveiligheid te maken had, kwam plotseling een einde in de tweede helft van de jaren tachtig, ten tijde van de *glasnost* en *perestrojka*.

De toenmalige KGB-voorzitter Vladimir Krjoetsjkov, wiens loopbaan een abrupt einde zou vinden door zijn prominente rol bij de mislukte staatsgreep tegen president Gorbatsjov in augustus 1991, liet zich regelmatig in de elektronische en geschreven media interviewen. Ook andere hoge KGB-functionarissen lieten zich niet onbetuigd. Over het algemeen waren de interviews met Krjoetsjkov en anderen echter weinig informatief. Ze hadden vooral tot doel het bestaansrecht van de KGB te legitimeren in een tijd dat het centrale gezag in de Sovjet-Unie steeds meer zijn greep op de politieke ontwikkelingen verloor.

Soms nam Krjoetsjkov het in zijn openbare uitspraken niet zo nauw met de waarheid. Zo ontkende hij in 1989 tijdens een zitting van de Opperste Sovjet van de USSR, het bestaan van een 'instituut van geheime informanten'. Op een vraag dienaangaande antwoordde hij ontwijkend. Hij deed het voorkomen alsof informanten door de KGB alleen ter bestrijding van spionage werden ingezet en niet tegen de eigen bevolking.

Hoewel er over de aantallen informanten waarover de KGB binnen de sovjetmaatschappij beschikte na 1991 nooit harde cijfers zijn vrijgegeven, mag men aannemen dat de KGB net als bijvoorbeeld het Oost-Duitse *Ministerium für Staatssicherheit* met zijn agenten en informanten alle geledingen van de sovjetmaatschappij had gepenetreerd. Tijdens dezelfde zitting van de Opperste Sovjet verklaarde Krjoetsjkov dat de KGB geen sovjetburgers afliuisterde tegen wie geen concrete beschuldiging was ingebracht of tegen wie geen verdenking bestond van samenwerking met een

buitenlandse inlichtingendienst of terroristische organisatie.<sup>3</sup>

De ongeloofwaardigheid van deze bewering bleek overduidelijk na de mislukte staatsgreep van augustus 1991. De openbare aanklager Valentin Stepankov, die het onderzoek naar de gebeurtenissen leidde, stelde toen vast dat de KGB al lange tijd vóór augustus 1991 tal van politici en andere sovjetburgers had afgeluisterd, onder wie de kapster van Raisa Gorbatsjov en de tennisleraar van Boris Jeltsin.

Hoewel Krjoetsjkov in augustus 1991 als KGB-voorzitter werd afgezet en van het politieke toneel verdween, werd nog onder zijn leiding een begin gemaakt met een selectieve opening van de KGB-archieven. Christopher Andrew en Vasili Mitrochin schrijven in *The Mitrokhin Archive* dat Krjoetsjkov in september 1990 een 'Besluit van de Voorzitter' deed uitgaan dat er 'meer gebruik gemaakt moest worden van archiefmateriaal' om een 'positief' beeld van de KGB en 'zijn meest beroemde zaken' voor het voetlicht te brengen. In veel gevallen werd daartoe een voor de KGB betrouwbare Russische auteur, vaak een KGB-officier, samengebracht met een gerenommeerde westerse auteur.

Dat door het beschikbaar stellen van KGB-materiaal aan westerse uitgeverijen ook nog de nodige harde valuta konden worden binnengehaald, zal ook ongetwijfeld een rol hebben gespeeld in de overwegingen van Krjoetsjkov en zijn opvolgers in Rusland na 1991. Het eerste boek dat op die manier ontstond was *Deadly Illusions* van de Britse auteur John Costello en de KGB-officier Oleg Tsarev, dat in 1993 verscheen.

De centrale figuur van het boek was de legendarische inlichtingsofficier van de NKVD, Alexander Orlov. Hij was NKVD-resident in Spanje ten tijde van de Spaanse burgeroorlog, toen hij in 1938 teruggeroepen werd naar Moskou. Hij voelde er niet voor zoals vele inlichtingsofficieren die toentertijd uit het buitenland werden teruggeroepen, bij terugkeer in Moskou van verraad te worden beschul-

digd en in de kelders van de Loebjanka (het hoofdkwartier van de NKVD) door een nekschot te worden geëxecuteerd.

Orlov ging daarom niet terug naar Moskou maar kwam in 1938 via Frankrijk in de Verenigde Staten terecht, waar hij in 1973 overleed. Bij zijn dood werd hij in de Verenigde Staten gezien als iemand die eind jaren dertig met het communisme gebroken had. Uit *Deadly Illusions* bleek dat dat maar zeer ten dele waar was. Zoals het een echte *spymaster* betaamt, had Orlov zijn belangrijkste geheimen altijd voor zich gehouden. Uit het Russische archiefmateriaal dat Costello en Tsarev konden gebruiken, bleek onder andere dat Orlov in de eerste helft van de jaren dertig als illegaal NKVD-resident in Londen een belangrijke rol had gespeeld bij de rekrutering van de legendarische vijf NKVD-agenten Anthony Blunt, Guy Burgess, John Cairncross, Donald Maclean en Kim Philby, die in de Engelstalige literatuur doorgaans worden aangeduid als *the Magnificent Five*.

Deze vijf agenten zouden tijdens hun carrière vitale posten binnen het Britse overheidsapparaat bekleden en Moskou informatie van onschatbare waarde leveren. Philby werd tijdens zijn periode bij de inlichtingendienst MI6 gezien als een *coming man* en toekomstig hoofd van de dienst. Als resident in Spanje, enkele jaren na de rekrutering van de vijf, onderhield Orlov ook enige tijd de verbinding met Philby, die toen als correspondent van *The Times* en NKVD-agent actief was in het nationalistische kamp. Ontmoetingen met Philby vonden plaats in Zuid-Frankrijk.

*Deadly Illusions* was een belangrijk boek omdat tal van bijzonderheden over de rekrutering en activiteiten van het legendarische vijftal hier voor de eerste maal werd onthuld. De rol van Orlov was nieuw en was bijvoorbeeld door Philby, in zijn vanuit Moskou geschreven zeer eenzijdige autobiografie *My Silent War*, verzwegen. *Deadly illusions* bevatte tevens zeer interessante informatie, aan Russi-

<sup>3</sup> *Sovetskaja Rossija (Sovjet Rusland)*, 17 juli 1989.

sche archieven ontleend, over de Berlijnse tak van het beroemde sovjet-spionagenetwerk tijdens de Tweede Wereldoorlog, de *Rote Kapelle*.

Ook boden de auteurs nieuws over de lotgevallen van de Britse anti-communistische 'activist' Sidney Reilly, die begin jaren twintig door de OGPOE, de inlichtingendienst van het Rode Leger, naar de Sovjet-Unie werd gelokt en daar werd geliquideerd.

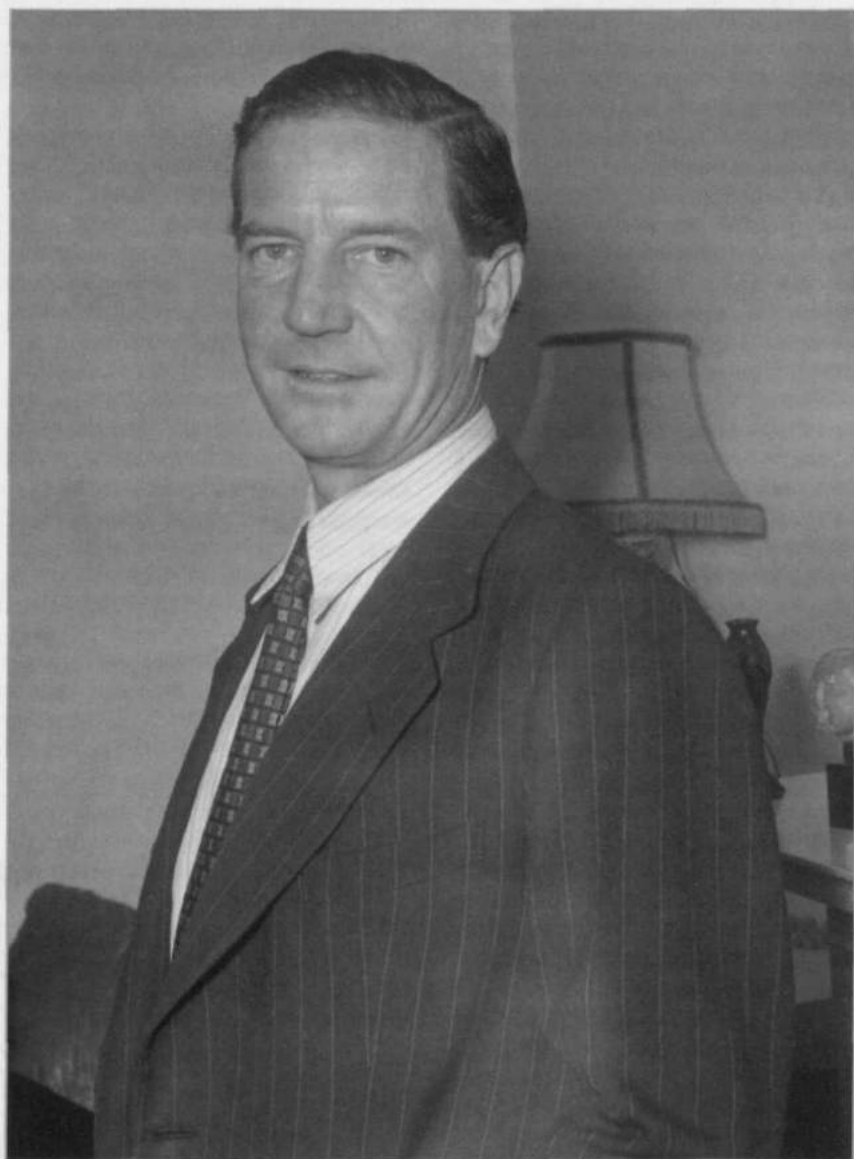
*Deadly Illusions* is niet zonder meer af te doen als een *public relations exercise* zoals in sommige reacties wel is beweerd. Ook een aantal minder frisse episodes uit de activiteiten van de NKVD in Spanje tijdens de burgeroorlog komen aan de orde, zoals de liquidatie van de leider van de Spaanse onafhankelijke marxistische partij POUM, Andrés Nin. Nin volgde allesbehalve slaafs de sovjetlijn tijdens de burgeroorlog en verdween in 1937 zonder dat zijn lijk ooit werd gevonden. In zijn verdwijning werd de hand van de NKVD vermoed.

Uit documenten die de Russische overheid voor *Deadly Illusions* beschikbaar stelde, blijkt overduidelijk de betrokkenheid van de NKVD bij de moord op Nin en waarschijnlijk ook die van Orlov persoonlijk.

### **The Crown Jewels**

In de loop van de jaren negentig werd *Deadly Illusions* gevolgd door andere publicaties die ook op in Moskou vrijgegeven materiaal over de *Magnificent Five* waren gebaseerd. Zo is er de meest actuele en volledige biografie van Philby, geschreven door Genrich Borovik, een Russische journalist die volgens de gewezen KGB-generaal Oleg Kaloegin (zie diens memoires *The First Directorate*) in het verleden menigmaal door de KGB gewenste berichten in de sovjetmedia heeft gelanceerd.

Een van de talrijke saillante details uit Boroviks Philby-biografie, is dat de door het vijftal aan Moskou geleverde informatie tijdens de Tweede Wereldoorlog dermate goed was, dat de Centrale ging twijfelen aan hun loya-



**Kim Philby** (Bron: Spaarnestad fotoarchief)

liteit. De geleverde informatie was zo onwaarschijnlijk goed dat de vijf gedurende enige jaren voor dubbelagenten van de Britse inlichtingendienst MI6 werden aangezien. Ook de mededeling van Philby dat MI6 tijdens de Tweede Wereldoorlog geen agenten binnen de Sovjet-Unie had, werd niet geloofd en versterkte het wantrouwen jegens hem.

De SVR stelde ook veel interessant archiefmateriaal beschikbaar voor een andere publicatie over het illustere vijftal, *The Crown Jewels* van Nigel West en dezelfde Oleg Tsarev,

dat in 1998 verscheen. Daarin wordt onder andere in een uitvoerige bijlage ingegaan op het soort informatie dat Philby aan de NKVD leverde. Er wordt ook de nodige aandacht besteed aan de activiteiten in de jaren dertig ten bate van de NKVD van de Nederlander Han Pieck, die doorgaans in Engelstalige publicaties over de KGB een bescheidener rol krijgt toebedeeld dan hij lijkt te verdienen. (De beschrijving van Piecks rol in het standaardwerk van Andrew en Gordievsky over de KGB uit 1990, *KGB. The Inside Story of Its Foreign Operations from Lenin to*

Gorbachev, is ronduit karig te noemen.) Het is ondoenlijk hierbij op de grote hoeveelheid nieuw materiaal dat in *The Crown Jewels* aan bod komt, in te gaan, maar één detail betreffende de befaamde NKVD-illegaal Arnold Deutsch is ronduit intrigerend. Deutsch heeft, zoals bekend, een sleutelrol gespeeld bij de rekrutering van de *Magnificent Five* in de eerste helft van de jaren dertig. Hij was immers degene die Philby het voorstel deed voor de Sovjet-Unie te gaan werken op een bank in het Londense Regent's Park in juni 1934.

Zoals de gewoonte was binnen de communistische beweging moest ook Deutsch van tijd tot tijd een 'biografie' (curriculum vitae) op schrift stellen en in die vorm aan hogere instanties binnen de NKVD over zichzelf rapporteren. Dergelijke rapportages waren ook een belangrijk veiligheidsmechanisme, omdat ze over tijd ook konden worden gebruikt om mogelijke tegenspraken in de verschillende

versies op te sporen. Die konden weer duiden, zo was de gedachte, op een gebrek aan loyaliteit of zelfs mogelijk verraad.

West en Tsarev citeren uitvoerig uit de biografie die Deutsch in 1938 voor zijn NKVD-superieuren schreef. Interessant genoeg zegt hij daarin over zichzelf, dat hij naast zijn kennis van andere Europese talen – hij sprak vloeiend Duits en Engels – ook Nederlands kon lezen en verstaan.

Als hij de waarheid sprak, lijkt de voor de hand liggende conclusie dat hij ook in Nederland voor de NKVD actief is geweest, hoewel daarvan tot nu toe niets concreets bekend is.

### Hiss, White en de Rosenbergs

Mede door het materiaal wat door de SVR de afgelopen jaren beschikbaar is gesteld voor publicaties bij westerse uitgeverijen, is er definitief zekerheid

gekomen over de beschuldigingen van spionage aan het adres van een aantal omstreden figuren uit de Amerikaanse geschiedenis ten tijde van de Koude Oorlog. De spionageactiviteiten van iemand als Alger Hiss, tot eind jaren veertig in een hoge functie werkzaam bij het State Department, zijn inmiddels niet meer te loochenen.<sup>4</sup> Hetzelfde geldt voor Harry

<sup>4</sup> Een van de vele pikante details uit de loopbaan van Hiss is dat hij in 1945 deel uitmaakte van de Amerikaanse delegatie bij de conferentie in Jalta. Het materiaal dat door de SVR over Hiss is vrijgegeven, is overigens relatief weinig omdat hij niet voor de KGB werkte, maar een agent was van de militaire inlichtingendienst GROE. In de GROE-archieven is dus het echte dossier van Hiss aan te treffen. De GROE heeft echter na 1991 niets uit zijn archieven prijs gegeven. Hoe verpletterend de bewijzen van Hiss' spionage voor de Sovjet-Unie zijn, blijkt het meest duidelijk uit het zeer gedetailleerde en meeslepende boek van Allen Weinstein, *Perjury*. Pikant is ook het feit dat Hiss tot aan zijn dood in 1996 zijn onschuld volhield.



De wereld zit er vol van

Dexter White, de hoge ambtenaar bij het Amerikaanse ministerie van Financiën tot aan zijn plotselinge dood in 1948.

Ook van het echtpaar Julius en Ethel Rosenberg dat in 1953 wegens spionage ter dood werd veroordeeld en geëxecuteerd, staat inmiddels onomstotelijk vast dat zij voor de KGB hebben gewerkt. De gepensioneerde KGB-officier Alexander Feklisov die in de jaren veertig geruime tijd de controller van Julius Rosenberg is geweest, gaat in zijn memoires uit 1999 uitvoerig in op de activiteiten van de Rosenbergs. Men kan zich afvragen of de mate waarin het echtpaar had gespioneerd een doodvonnis rechtvaardigde, speciaal in het geval van Ethel Rosenberg, maar dat is een andere kwestie.

Met name voor de Rosenbergs en Alger Hiss gold dat zij tijdens de Koude Oorlog de inzet waren van een heftige controverse over de vraag of zij zich wel echt aan spionage schuldig hadden gemaakt. Velen, vooral aan de linkerzijde van het Amerikaanse politieke spectrum, hebben jarenlang luidruchtig blijk gegeven van hun overtuiging dat Hiss en de Rosenbergs het slachtoffer waren van een anti-communistische heksenjacht.

Materiaal betreffende Hiss, White, de Rosenbergs en vele andere Amerikanen die voor de Sovjet-Unie als agent werkzaam zijn geweest in de jaren dertig en veertig, is door de huidige Russische overheid vrijgegeven voor publicatie in *The Haunted Wood*, dat in 1999 verscheen. Ook hier was weer sprake van een co-productie van een westerse en een Russische auteur: Allen Weinstein en de voormalige KGB-officier Alexander Vassiliev.

Het door de Amerikaanse afluister- en decodeerdienst *National Security Agency* in de loop van de jaren negentig vrijgegeven *Venona*-materiaal, leverde nog eens uit andere hoek een bevestiging op van de strekking van *The Haunted Wood*. *Venona* was de codenaam van het tot voor kort geheime project dat tot doel had gecodeerde berichten van de NKVD en in mindere mate de GROE, verstuurd vanuit

en naar Moskou in 1940-1948, te ontcijferen en te lezen.

Amerikaanse overheidsinstanties zijn nog tijdens de Tweede Wereldoorlog, in 1943, aan het project begonnen en hebben het pas officieel in 1980 afgesloten. *Venona* was slechts gedeeltelijk succesvol en vele berichten konden maar zeer ten dele of helemaal niet worden ontcijferd, waardoor vele NKVD-agenten onontdekt bleven. Dat blijkt onder andere uit het boek *Venona* van de Amerikaanse historici Haynes en Klehr.

De strekking van het *Venona*-materiaal en *The Haunted Wood* kwam echter op hetzelfde neer: het Amerikaanse overheidsapparaat was in de jaren dertig en veertig op grote schaal door de NKVD en de GROE gepenetreerd. Tal van agenten, naast de al genoemde Hiss, de Rosenbergs en White, zijn bij naam en toenaam zowel in *The Haunted Wood* als in *Venona* terug te vinden.

Op de betrouwbaarheid van de informatie die door de Russische overheid voor de hierboven genoemde publicaties aan westerse uitgevers ter beschikking is gesteld, is over het algemeen niet veel aan te merken. Er zijn althans schrijver dezes geen voorbeelden bekend uit genoemde boeken waarin feiten worden gepresenteerd, ontleend aan Russisch archiefmateriaal, die aantoonbaar onjuist zijn. Anders is het gesteld met de volledigheid van het materiaal.

De auteurs in kwestie hebben niet zelf de selectie gemaakt in de KGB-archieven. In een aantal gevallen gaat het zoals gezegd om een voormalige KGB-officier die is gekoppeld aan een westerse auteur, die zelf geen Russisch leest. Dat laatste is het geval bij overigens gerenommeerde auteurs zoals John Costello, Allen Weinstein en Nigel West. Dat dergelijke auteurs niet zelf de selectie hebben gemaakt is dus evident.

Maar zelfs voor auteurs met een KGB-achtergrond zoals Vassiliev en Tsarev, geldt ongetwijfeld dat het materiaal dat zij voor hun publicatie hebben gebruikt door de SVR is gefiatteerd.

Andrew en Mitrochin hebben erop gewezen dat soms bepaalde gegevens zijn weggelaten. Diverse westerse auteurs, onder wie Genrich Borovik, John Costello en Nigel West, hebben inmiddels materiaal uit het omvangrijke Philby-dossier van de SVR ontvangen.

Eén episode is daarbij echter telkens buiten beschouwing gelaten. De zaak speelde in 1951 toen Philby zich op het hoogtepunt van zijn carrière bij MI6 bevond en *chief of station* in Washington was. Door de ontsnapping van Guy Burgess en Donald Maclean vanuit Engeland naar Moskou kwam Philby ernstig in verlegenheid, omdat hij dacht dat de verdenking vervolgens op hem zou vallen, hetgeen inderdaad zou gebeuren. Op dat belangrijke moment werden geld en instructies voor Philby op de verkeerde plaats voor hem gereed gelegd.

Er traden ook spanningen op met zijn KGB-controller, die vervolgens op oneervolle wijze naar Moskou werd teruggeroepen. Geen van de hier genoemde boeken maakt melding van deze voor de KGB pijnlijke episode. Uitzondering is *The Mitrokhin Archive*, dat echter zoals hierna nog ter sprake zal komen, zonder toestemming van Moskou is verschenen.

### Weinig over interne repressie en controle na 1953

Hoe selectief de Russische overheid in zijn vrijgave van materiaal uit de KGB-archieven te werk gaat, wordt duidelijk als men ziet welke thema's buiten beschouwing blijven. Het merendeel van het materiaal dat aan westerse historici en uitgevers ter beschikking is gesteld, heeft betrekking op de triomfen van de buitenlandse inlichtingendienst van de NKVD/KGB, met name in de jaren dertig en veertig. Ook over de bloedige zuiveringen en de *Goelag* onder Stalin is het nodige vrijgegeven. Opvallend is echter dat de manier waarop de KGB binnen de USSR func-

tioneerde na 1953 en de daaraan gekoppelde systematische repressie, vrijwel volledig buiten beschouwing is gebleven.

Over de vervolging van dissidenten en de mate waarin de KGB alle sectoren van de sovjetmaatschappij met agenten had gepenetreerd, is de afgelopen tien jaar door de Russische overheid een diep stilzwijgen bewaard. Ook in memoires van KGB'ers die in die periode zijn verschenen worden dergelijke thema's nauwelijks behandeld.

Typend zijn in dit verband de herinneringen van de KGB-officier Filipp Bobkov, die in de Brezjnef-tijd hoge functies bekleedde bij het beruchte Vijfde Hoofddirectoraat van de KGB, dat verantwoordelijk was voor de vervolging van dissidenten. Tot 1991 was Bobkov ook nog op andere hoge posten bij de KGB actief. In zijn memoires *KGB i vlast (De KGB en de macht)* ontkent hij glashard dat er in de Sovjet-Unie dissidenten werden vervolgd. Ook het Vijfde Hoofddirectoraat van de KGB waarbinnen hij zelf zo'n belangrijke rol speelde, vervolgde geen dissidenten, zo beweert hij. Volgens hem ging het Vijfde Hoofddirectoraat slechts tot repressieve maatregelen over in het geval van 'ernstige onwettige handelingen'.

In een artikel uit 1998 pleegde hij een soort woordenspel door te beweren dat zijn directoraat zich niet richtte tegen andersdenkenden, maar tegen hen die 'zich uitspraken tegen de toen bestaande constitutionele orde en actief uit waren op de ondermijning ervan.' Het zal niet verbazen dat Bobkov ook het bestaan van misbruik van de psychiatrie in de Sovjet-Unie in zijn memoires ontkent. Ook rept hij met geen woord over het werken met informanten door de KGB binnen de dissidentenbeweging en de kerken. Onder andere uit *The Mitrokhin Archive* is inmiddels genoegzaam bekend dat dat op grote schaal gebeurde. Zo had de KGB de kerken in de USSR, met name de Russisch Orthodoxe Kerk, met tal van agenten en informanten gepenetreerd. Onder

andere Aleksii II, vanaf 1990 Patriarch van de Russisch Orthodoxe Kerk, was in de sovjetperiode onder de code-naam *Drozdoz* jarenlang een agent van de KGB. Hij had voor zijn KGB-werk zelfs in het geheim een hoge onderscheiding ontvangen.

Het belang van dergelijke agenten voor de KGB was overigens niet alleen dat zij informatie verschaften. Zij waren eventueel ook in staat het beleid van de kerk in een voor de KGB en de Sovjet-Unie gunstige zin te beïnvloeden. Het eindresultaat was dat de Russisch Orthodoxe Kerk als onafhankelijke instelling feitelijk niet bestond en aan het sovjetregime ondergeschikt werd gemaakt.

Hoezeer de KGB de sovjetmaatschappij in zijn greep hield en alles en iedereen bespioneerde, wordt duidelijk uit een passage uit de memoires van de voormalige KGB-generaal Oleg Kalugin, die inmiddels in de Verenigde Staten woont en zich vaak kritisch over zijn vroegere werkgever heeft uitgelaten. Over zijn tijd bij de KGB in Leningrad begin jaren tachtig schrijft hij:

*'I was one of three KGB officials in Leningrad with the power to authorize wiretapping in the city. As I spent more time on the job, I marvelled at the extent of our bugging, surveillance, and mail interception efforts. In the Big House (het KGB-hoofdkwartier in Leningrad), nearly one thousand KGB employees, working in a warren of rooms, were involved around the clock in monitoring and recording phone wiretaps and other bugs. At any given time, there were dozens of phones, offices, and apartments being bugged, and this battalion of KGB workers - most of them women - recorded and transcribed the conversations. Sitting in the Big House, we had the capacity, through special hook-ups with the central Leningrad phone station, to record any conversation in the city. The phone calls of dissidents, artists and other troublemakers were monitored periodically. Foreign diplomats,*

*businessmen and journalists were subjected to near-constant bugging of their phones and hotel rooms. Indeed, at the major Intourist hotels - the Astoria, Evropeyskaya, and Pribaltiskaya - suspicious foreigners were placed in certain rooms already outfitted with hidden microphones. Tourists also were watched, though more spottily since there were so many of them. Virtually all the Intourist guides were KGB informers, who immediately reported to us, if they harbored suspicions about a certain foreign tourist.'*<sup>5</sup>

Al dit werk leverde volgens Kalugin als het om spionage ging nauwelijks iets op. Een enkel belastend feit over huwelijksontrouw of homoseksualiteit kwam aldus aan het licht. Dat kon dan eventueel gebruikt worden om iemand tot samenwerking met de KGB te dwingen, als dat nodig mocht zijn. Dit stond echter niet in verhouding tot de kolossale krachtsinspanning die door de KGB werd geleverd. Diverse KGB-overlopers, die in de loop der jaren naar het Westen zijn gekomen en hun memoires hebben geschreven, schetsen een beeld van het toezicht van de KGB op de sovjetmaatschappij, dat niet wezenlijk van dat van Kalugin afwijkt.

Een verschijnsel dat in memoires en andere publicaties in Rusland na 1991 ook vrijwel niet aan de orde komt (en uiteraard ook niet in boeken over de KGB die bij westerse uitgeverijen zijn verschenen) is dat van de zogeheten 'officieren van de actieve reserve' (*ofitsery dejstvoejojsejtsjego reserva*). Dat was een van de talrijke manieren waarop de KGB namens het communistische regime de maatschappij onder controle hield. Het ging daarbij om KGB-officieren die onder een dekmantel bij andere organisaties op sleutelposities werden geplaatst. Zij fungeerden niet alleen als 'elite-informanten', maar poogden ook de orga-

<sup>5</sup> Kalugin, O. *The First Directorate* (New York, 1994), 297-298.

nisaties in de door de KGB gewenste richting te beïnvloeden. (Daarnaast waren er nog 'gewone' informanten, die niet bij de KGB in vaste dienst waren. Hierover zijn ook na 1991 nooit cijfers vrijgegeven.) De inlichtingenafdeling van de KGB, het Eerste Hoofddirectoraat, plaatste zijn medewerkers onder diplomatieke dekman- tel als officieren van de actieve reserve op ambassades in het buitenland. Dat was een bekend verschijnsel, maar over de manier waarop het instituut van de officieren van de actieve reserve binnen de Sovjet-Unie functioneerde, bewaren vrijwel alle ex-KGB'ers in hun publicaties een hardnekkig stilzwijgen.

Eén van de weinigen die erover heeft geschreven, is Jevgeni Grig (een pseudoniem). Grig werd in het midden van de jaren zeventig vanuit het Vijfde Hoofddirectoraat ondergebracht bij de VAAP (Al-Unie Bureau voor Auteursrechten). In 1987 werd hij overgeplaatst naar de uitgeverij Goskomizdat. De positie die Grig bij VAAP bekleedde was voor de KGB van belang vanwege de veelvuldige contacten die hij daardoor onderhield met buitenlandse schrijvers en uitgevers die in de Sovjet-Unie wilden publiceren en met sovjetschrijvers die hun werk in het buitenland wilden uitbrengen.

Grig hield de schrijvers en uitgevers niet alleen in de gaten. Als het zo uitkwam kon hij ze ook als informanten rekruteren. Schrijvers werden, net als kunstenaars, als potentieel zeer staatsgevaarlijk beschouwd. Volgens Grig beschikte de KGB binnen de Schrijversbond en organisaties voor componisten en architecten, over een 'niet gering' aantal agen-

ten. (Agenten waren informanten, die dus niet bij de KGB in vaste dienst waren.) Hij geeft echter geen cijfers. Bij VAAP waren in de tijd dat Grig daar werkte, vijf tot zeven KGB-officieren van de actieve reserve ondergebracht. Ook de vice-voorzitter van VAAP was op een zeker moment een KGB-officier. Officieren van de actieve reserve kregen hun salaris van de KGB doorbetaald. Eventuele extra inkomsten van hun tweede werkgever moesten ze afdragen. Hun eerste loyaliteit lag bij de KGB. Grig ging ongeveer één keer per week voor overleg langs bij het hoofdkwartier van de KGB, de Loebjanka. Vanzelfsprekend werden

zijn collega's bij VAAP niet geacht op de hoogte te zijn van zijn werkzaamheden voor de staatsveiligheidsdienst.

Grig kwam er ook werken met een zogenaemde 'legende', dat wil zeggen een fictieve loopbaan voor de periode voorafgaande aan zijn werk bij VAAP.

### Ontvoeringen, moorden en andere affaires

Een periode waarover men traditioneel ook ten tijde van de Sovjet-Unie een diep stilzwijgen bewaarde was augustus 1939-juni 1941, de tijd van het bondgenootschap met nazi-Duitsland. Het zou voor hedendaagse historici bijvoorbeeld interessant zijn te weten op welke punten er in die jaren sprake is geweest van samenwerking tussen de veiligheidsdiensten van nazi-Duitsland en de Sovjet-Unie.

Het is bekend dat er toen gevangene Duitse communisten, die eerder in het kader van de zuiveringen onder Stalin waren gearresteerd, uit de Goelag door de NKVD aan de Gestapo zijn overgedragen. Een van de slachtoffers was Margarete Buber-Neumann, die daarover in haar herinneringen *Als Gefangene bei Stalin und Hitler*, verslag heeft gedaan. De Poolse generaal Bor-Komorowski heeft geschreven, dat afvaardigingen van de Gestapo en de NKVD begin 1940 enkele weken lang in Krakau bijeenkwamen om de coördinatie van operaties tegen het Poolse verzet te bespreken.

De huidige Russische overheid heeft zoals te verwachten was, geen opening van zaken gegeven over de contacten met Duitse veiligheidsdiensten in deze periode en het is ook niet waarschijnlijk dat dat in de naaste toekomst zal gebeuren.

Een beschrijving van de geschiedenis van de sovjetinlichtingendienst kan natuurlijk niet heen om de talloze moordaanslagen en ontvoeringen, die in de jaren voor en na de Tweede Wereldoorlog door die dienst in het



De universele agent

buitenland zijn gepleegd. Daarbij waren voornamelijk, maar niet uitsluitend, Russische emigranten en afvallige sovjetcommunisten het slachtoffer, met als bekendste voorbeeld Trotski in augustus 1940 in Mexico.

Het derde deel van de *Essays over de geschiedenis van de Russische buitenlandse inlichtingendienst*, dat in 1997 in een oplage van tienduizend is gepubliceerd en geschreven door een auteurscollectief van de SVR, gaat inderdaad in op een aantal van dergelijke moorden en ontvoeringen. Onder andere de moord op Trotski wordt behandeld. Daarbij moet men echter bedenken dat de betrokkenheid van de NKVD bij de moord op Trotski al sinds jaar en dag bekend is en ook uitvoerig ter sprake komt in de in 1994 verschenen memoires van Pavel Sudoplatov. In de publicatie van de SVR wordt verrassend genoeg de nadruk gelegd op de bijdrage van Trotski en de trotskisten aan het verschijnsel van het 'anti-sovjetisme, dat vele jaren lang schade heeft berokkend aan de binnenlandse en buitenlandse politiek van de USSR en eveneens aan de internationale arbeiders- en communistische beweging'.

Ook wordt er gesuggereerd dat de trotskisten een dankbaar rekruterings-terrein vormden voor westerse inlichtingendiensten. Men krijgt de indruk dat de auteurs deze twee punten beschouwen als verzachtende omstandigheden bij de liquidatie van de leider van de Vierde Internationale. Heel vreemd gaan de auteurs ook te werk als het optreden van de NKVD tijdens de Spaanse burgeroorlog ter sprake komt. De naam van de leider van de 'trotskistische' partij POUM, Andrés Nin, valt wel, maar over zijn verdwijning en de betrokkenheid van de NKVD daarbij wordt met geen woord gerept. Dit in tegenstelling tot wat de auteurs van *Deadly Illusions*, zoals gezegd, enkele jaren eerder hadden geschreven over het einde van Nin.

Hoe moeilijk het voor de SVR is om opening van zaken te geven over het duistere verleden van de KGB/NKVD,



**Paraplu-  
moord op  
Georgi  
Markov**  
(Bron:  
Spaarnestad  
fotoarchief)

bewijst het geval van de inlichtingen-officier Stanislav Vaoepsjasov. In het biografisch woordenboek *Veterany vnesnej razvedki Rossii (Veteranen van de buitenlandse inlichtingendienst van Rusland)* dat in 1995 onder auspiciën van de SVR in Moskou verscheen, is ook een biografische schets van Vaoepsjasov opgenomen, waarin in het kort melding wordt gemaakt van het feit dat hij onder meer tijdens de Spaanse burgeroorlog voor de NKVD actief was.

Uit *The Mitrokhin Archive* blijkt hoe incompleet die beschrijving van Vaoepsjasovs carrière was. Het feit dat hij in Spanje betrokken was bij de aanleg en bewaking van een geheim crematorium, waarin de stoffelijke resten van slachtoffers van de NKVD werden verbrand, blijft in de SVR-publicatie uit 1995 onvermeld. Ook

wordt er niet gezegd dat Vaoepsjasov eind jaren twintig, in een eerdere fase van zijn carrière bij de NKVD, ter dood was veroordeeld wegens moord op een collega. Dat vonnis werd al gauw in een gevangenisstraf omgezet en hij werd later vrijgelaten om de draad van zijn loopbaan weer op te pakken. In een recenter verleden was er de beruchte 'papaplummoord' op de Bulgaarse balling Georgi Markov in Londen in 1978. Markov was onder meer werkzaam voor de BBC en het in München gevestigde *Radio Liberty*. Hij uitte tijdens uitzendingen herhaaldelijk kritiek op het communisme in Oost-Europa, in het bijzonder in zijn geboorteland Bulgarije. Terwijl hij in Londen bij de Tower Bridge op de bus stond te wachten, kwam hij in aanraking met een onbekende met een paraplu in de hand. Later op de dag werd hij ernstig ziek en enkele dagen

later overleed hij. Na zijn dood werd een kleine capsule met het dodelijk gif *ricine* uit zijn dijbeen verwijderd. Men speculeerde dat de capsule door de onbekende met de paraplu op Markov was 'afgevuurd'. Al gauw rees het vermoeden dat hij door de Bulgaarse geheime dienst, al dan niet in samenwerking met de KGB, was vermoord.

De enige voormalige KGB'er die in zijn memoires iets over deze affaire zegt, is Oleg Kalugin. Hij zegt in *The First Directorate*, begin 1978 aanwezig te zijn geweest bij een vergadering in de Loebjanka, het hoofdkwartier van de KGB, waarbij de KGB-top besloot de Bulgaren op hun verzoek technische steun te verlenen bij de liquidatie van Markov. Bij de vergadering waren volgens Kalugin naast hemzelf onder meer KGB-voorzitter

Joeri Andropov aanwezig en de latere voorzitter Vladimir Krjoetsjkov. Deze versie van Kalugin is op zich niet onaannemelijk, maar nooit uit andere bron bevestigd.

Het opvallende is dat ook Krjoetsjkov in zijn twee delen memoires, samen goed voor zo'n achthonderd bladzijden, er met geen woord over rept. Dat is des te merkwaardiger omdat hij erg gebeten is op Kaloegin – dat gevoel is overigens wederzijds – en dus alle reden heeft om hem op dit punt op z'n minst tegen te spreken.

Dat het voor het personeel van Russische diensten niet eenvoudig is zich van het bloedige verleden te distantiëren, blijkt ook uit een gebeurtenis die zich in 1993 voordeed. De voormalige hoge NKVD-officier Pavel Soedoplatov werd in dat jaar bij een bijeenkomst van de inlichtingendienst

SVR uitgenodigd. Soedoplatov was tijdens zijn carrière in de jaren dertig en veertig bij tal van smerige zaken betrokken en voerde onder andere persoonlijk de moordaanslag uit op de Oekraïense nationalistische leider Jevhen Konovalts in mei 1938 in Rotterdam. Tevens was hij vanuit Moskou het brein achter de operatie tegen Trotski in Mexico in 1940, die met diens dood eindigde.

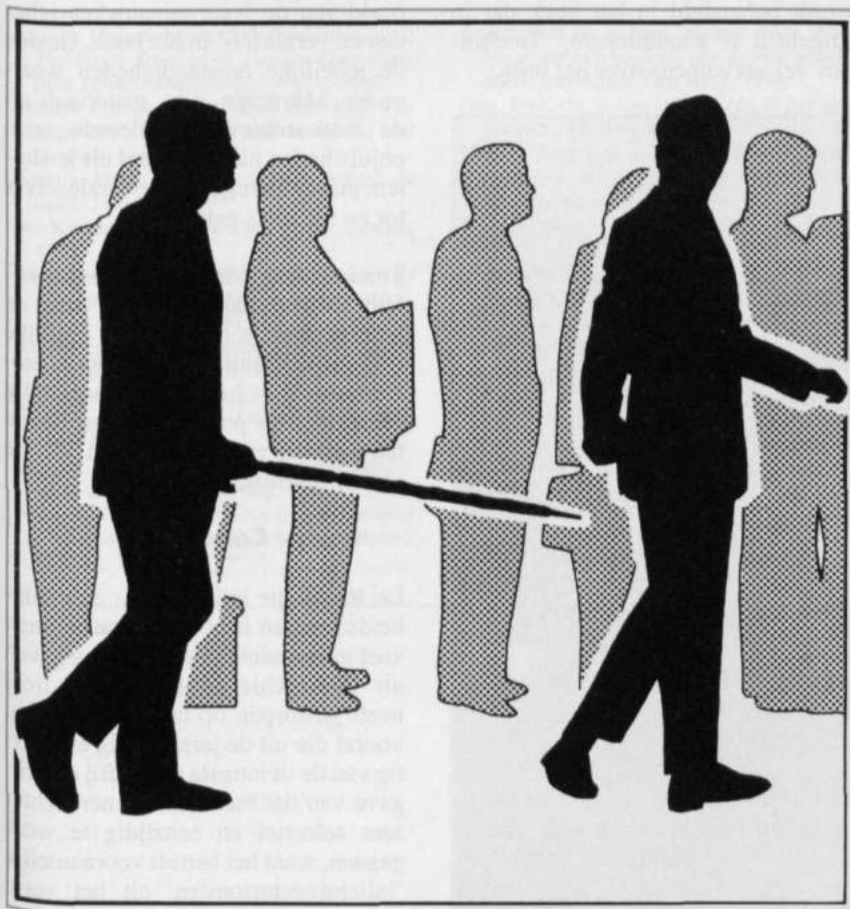
Soedoplatov kreeg bij binnenkomst van het aanwezige personeel van de SVR een staande ovatie die enkele minuten duurde.<sup>6</sup>

### Reactie op The Mitrokhin Archive

Hoe moeilijk het voor de huidige Russische diensten is het vaak onverkwikkelijke KGB-verleden onder ogen te zien, blijkt uit de reactie op de publicatie in het Westen van *The Mitrokhin Archive* of, liever gezegd, vooral uit het uitblijven daarvan. Dat boek is onder andere belangrijk, omdat het naast gegevens over talloze inlichtingenoperaties in het Westen, vele details bevat over de wijd vertakte penetratie met informanten van de kerken en de dissidentenbeweging in de Sovjet-Unie door de KGB. Dat zijn zoals gezegd thema's waarover de Russische overheid een diep stilzwijgen in acht neemt.

Daarnaast is *The Mitrokhin Archive* onder meer interessant omdat er veel informatie in te vinden is over de inzet van illegalen in Oost-Europa, vooral tegen de dissidentenbeweging in landen als Tsjechoslowakije en Polen. Die illegalen opereerden onder een valse identiteit en gaven zich tegenover Oost-Europese dissidenten veelal uit voor West-Europeanen die met hen sympathiseerden, om aldus allerlei informatie los te krijgen.

Al dit materiaal en nog veel meer was door de KGB-officier Vasili Mitrochin in zijn functie als archivaris bij het Eerste Hoofddirectoraat van de KGB, de inlichtingendienst, tot aan zijn



Paraplumoord (Bron: Spaarnestad fotoarchief)

<sup>6</sup> *Izvestija (Nieuws)*, 30 april 1994.



pensionering in 1985 gekopieerd. Hij deed dat in het diepste geheim en met groot persoonlijk risico. Hij werd daarbij naar eigen zeggen gemotiveerd door zijn afkeer van de KGB en het sovjetregime. In 1992 werd hij door de Britse inlichtingendienst MI6 met zijn gezin en de informatie die hij had verzameld, naar het Westen 'geëxfiltreerd'. Een groot deel van het materiaal dat Mitrochin meenam naar het Westen, zij het niet alles, is in *The Mitrokhin Archive* verwerkt, waarvan de Britse historicus Christopher Andrew de co-auteur is.

Na de verschijning van het boek in september 1999 heerste er vanuit Moskou enige tijd een oorverdovende stilte. Diverse personen in Moskou hebben rond die tijd ongetwijfeld menige slapeloze nacht gehad, vanwege de grote hoeveelheid waardevolle informatie die Mitrochin had meegenomen en gepubliceerd. Uiteindelijk kwam er een korte reactie van niemand minder dan de toenmalige

directeur van de SVR, Vjatsjeslav Troebnikov. (In het voorjaar van 2000 werd Troebnikov van zijn functie ontheven en overgeplaatst naar het ministerie van Buitenlandse Zaken. Hij werd opgevolgd door Sergej Lebedev.)

Op 22 december 1999 verscheen er een interview met Troebnikov in de *Izvestia*. Daarin bevestigde hij dat Mitrochin werkzaam was geweest bij het Eerste Hoofddirectoraat van de KGB. Hij zei dat Mitrochin 'een onbelangrijke functie had en vijftien jaar geleden om leeftijdsredenen was ontslagen in de rang van majoor.' Vervolgens zei hij dat de SVR na publicatie van het 'zogenaamde Mitrochin-archief' een onderzoek had ingesteld: 'Daaruit bleek dat een "Mitrochin-archief" in de echte zin van het woord niet bestond. Deze man had geen ruime toegang tot het materiaal dat wordt behandeld in het boek dat in Engeland is gepubliceerd.' Troebnikov zei vervolgens over het boek:

*Naar onze mening bevat het vele onnauwkeurigheden en verzinsels. Over sommige feiten wordt informatie gegeven die buitenlandse speciale diensten (dat wil zeggen inlichtingendiensten) bekend is geworden door Gordievsky en andere verraders. Het boek bevat geen documenten zoals de auteurs zelf erkennen. In verband met dit boek wil ik het woord betrouwbaarheid niet in de mond nemen en dus ook niet van schade (aan de SVR) spreken.*

Dit was een ouderwetse sovjetreactie. Troebnikov probeerde een 'probleem' op te lossen door simpelweg het bestaan ervan te ontkennen en de boodschapper, in dit geval Mitrochin, in discrediet te brengen door hem te betichten van het debiteren van onnauwkeurigheden en verzinsels. In het interview gaf hij geen enkel voorbeeld van de 'vele onnauwkeurigheden en verzinsels' in het boek. Gezien de moeilijke omstandigheden waaronder Mitrochin zijn materiaal uit de KGB-archieven kopieerde, zijn onjuistheden niet helemaal uit te sluiten, maar van regelrechte verzinsels is tot nu toe niets gebleken.

Troebnikovs reactie heeft ongetwijfeld alles te maken met het voor de huidige Russische diensten pijnlijke feit, dat de publicatie van *The Mitrokhin Archive* het eigen zorgvuldig geregisseerde public relations-beleid ten aanzien van het verleden van de KGB doorkruist.

### **Conclusie**

De Russische inlichtingen- en veiligheidsdiensten hebben de laatste jaren veel interessant materiaal vrijgegeven uit KGB-archieven dat nieuw licht heeft geworpen op tal van operaties, vooral die uit de jaren dertig en veertig van de twintigste eeuw. Bij de vrijgave van dat materiaal is men echter zeer selectief en eenzijdig te werk gegaan, want het betreft voornamelijk 'inlichtingentriomfen' uit het verre verleden. Op die manier hoopt men het prestige en de legitimiteit van de hui-



Het KGB-hoofdkwartier (Bron: abc-press)

dige Russische diensten te vergroten. Na 1991 zijn er in Rusland enkele tientallen memoires van voormalige KGB-officieren verschenen, die echter qua informatiegehalte doorgaans teleurstellen. Gevoelige thema's zoals die bijvoorbeeld in *The Mitrokhin Archive* uitvoerig aan de orde komen, worden daar zelden behandeld. Op zich is dat ook niet verwonderlijk want de meeste memoireschrijvers van de KGB, die na 1991 in Rusland zijn gebleven, hebben tijdens hun carrière de KGB en de Sovjet-Unie altijd trouw geëdiend.

De Russische openheid over het verleden van de eigen inlichtingen- en veiligheidsdiensten, hoe selectief ook, steekt overigens nog gunstig af

ten opzichte van het gevolgd beleid in enkele westerse landen. In het Verenigd Koninkrijk werkt de overheid aan publicaties op dit terrein slechts mondjesmaat mee en de publicatie van memoires van personeel van de diensten staat nog in de kinderschoenen.

Het feit dat de voormalige directeur-generaal van MI5, Stella Rington, binnenkort met toestemming van de Britse overheid haar memoires zal publiceren, is een revolutionaire gebeurtenis. Ook in Nederland toont de overheid zich op het punt van geschiedschrijving weinig coöperatief, als we afzien van publicaties als Engelens *Geschiedenis van de Binnenlandse Veiligheidsdienst* uit 1995.








Engelen is echter, zoals bekend, zelf werkzaam bij de BVD.

Toen 'buitenstaanders' als Cees Wiebes en Bob de Graaff zich met de geschiedschrijving van de Inlichtingendienst Buitenland gingen bezighouden, wat uiteindelijk resulteerde in de publicatie van *Villa Maarheeze*, konden zij rekenen op krachtige tegenwerking van de Nederlandse overheid. Pas in een later stadium toonde men zich enigszins coöperatief. Memoires van ex-medewerkers van BVD of MID zijn hier te lande een onbekend verschijnsel. Nederland kan dus merkwaardig genoeg, op het punt van openheid over het verleden van de diensten, in zekere zin nog een voorbeeld aan Rusland nemen.

#### Literatuur

- Andrew, Christopher en Oleg Gordievsky. *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. Londen, 1990.
- Andrew, Christopher en Vasili Mitrokhin. *The Mitrokhin Archive. The KGB in Europe and the West*. Londen, 1999.
- Bobkov, Filipp. *KGB i vlast. (De KGB en de macht.)* Moskou, 1995.
- Bor-Komorowski, T. *The Secret Army*. Londen, 1950.
- Borovik, Genrikh. *The Philby File. The Secret Life of the Master Spy - KGB Archives Revealed*. Londen, 1994.
- Buber-Neumann, Margarete. *Als Gefangene bei Stalin und Hitler. Eine Welt im Dunkel*. Stuttgart, 1985 (oorspr. 1949).
- Costello, John en Oleg Tsarev. *Deadly Illusions*. Londen, 1993.
- Engelen, D. *Geschiedenis van de Binnenlandse Veiligheidsdienst*. Den Haag, 1995.
- Feklisov, Alexander. *Priznanije razvedsjika (Bekentenis van een inlichtingenofficier)*. Moskou, 1999.
- Graaff, Bob de & Cees Wiebes, *Villa Maarheeze. De geschiedenis van de Inlichtingendienst Buitenland*. Den Haag, 1999.
- Grig, Jevg. *Da, ja tam rabotal. (Ja, ik heb daar gewerkt.)* Moskou, 1997.
- Haynes, John Earl en Harvey Klehr, *Venona. Decoding Soviet Espionage in America*. New Haven en Londen, 1999.
- Kalugin, Oleg. *The First Directorate. My 32 Years in Intelligence and Espionage Against the West*. New York, 1994.
- Krjoetsjkov, Vladimir. *Litsjnoje delo. Tsjast pervaja, tsjast vtoraja. (Persoonlijk dossier. Deel een, deel twee.)* Moskou, 1996.
- Otsjerki istorii rossijskoj vnesnej razvedki. *Tom 3, 1933-1941 gody. (Essays over de geschiedenis van de Russische buitenlandse inlichtingendienst. Deel 3, de jaren 1933-1941)* Moskou, 1997.
- Philby, Kim. *My Silent War*. Londen, 1983 (oorspr. 1968).
- Sloezjba vnesnej razvedki Rossijskoj Federatsii. *Veterany vnesnej razvedki Rossii (Kratki biografitsjeskispravotsjnik)*[Buitenlandse Inlichtingendienst van de Russische Federatie. Veteranen van de buitenlandse inlichtingendienst van Rusland.(Kort biografisch naslagwerk)] Moskou, 1995.
- Stepankow, Valentin. *Das Kreml-Komplott. Putschisten, Drahtzieher, Hintermänner. Die Beweise des Generalstaatsanwalts*. München, 1992.
- Sudoplatov, Pavel and Anatoli Sudoplatov, with Jerrold L. and Leona P. Schecter. *Special Tasks. The Memoirs of an Unwanted Witness - A Soviet Spymaster*. Boston, 1994.
- Weinstein, Allen. *Perjury: The Hiss-Chambers Case*. New York, 1997 (updated edition).
- Weinstein, Allen en Alexander Vassiliev, *The Haunted Wood: Soviet Espionage in America - The Stalin Era*. New York, 1999.
- West, Nigel en Oleg Tsarev. *The Crown Jewels. The British Secrets at the Heart of the KGB Archives*. Londen, 1998.

**Inlichtingen- en Veiligheidsdiensten NAVO- partners (incl. Israël en Zweden)**

<b>BELGIE</b> 	Federal Intelligence and Security Agency ( <i>SV</i> ) (C / V) Military Intelligence and Security Agency ( <i>SGR</i> ) (M / VI)	<b>ITALIE</b> 	Servizio per le Informazioni e la Sicurezza Democratica ( <i>SISD</i> ) (C / VI) Servizio per le Informazioni e la Sicurezza Militare ( <i>SISMI</i> ) (M / VI)
<b>CANADA</b> 	Privy Council Office ( <i>PCO</i> ) (C / VI) Security Intelligence Review Committee ( <i>SIRC</i> ) (C / VI) Canadian Security Intelligence Service ( <i>CSIS</i> ) (C / VI) Communications Security Establishment ( <i>CSE</i> ) (M / I) Royal Canadian Mounted Police ( <i>RCMP</i> ) (C / V) Criminal Intelligence Service Canada ( <i>CSIC</i> ) (C / VI)	<b>NEDERLAND</b> 	Binnenlandse Veiligheidsdienst ( <i>BVD: National Security Service</i> ) (C / VI) Militaire Inlichtingendienst ( <i>MID: Military Intelligence Service</i> ) (M / VI)
<b>DENEMARKEN</b> 	Danish Defence Intelligence Service ( <i>DDIS</i> ) (M / I)	<b>NOORWEGEN</b> 	Kontrollutvalget for overvåkings- og sikkerhetstjenesten ( <i>Control Committee for the Intelligence and Security Services</i> ) (C / VI) Forsvarets sikkerhetstjeneste ( <i>Joint Defence Security Service</i> ) (M / V) Forsvarets etterretningstjeneste ( <i>Joint Defence Intelligence Service</i> ) (M / I) Politiets overvåkingstjeneste ( <i>Police Intelligence Service</i> ) (C / VI)
<b>DUITSLAND</b> 	Bundes Nachrichten Dienst ( <i>BND</i> ) (C / I) Bundesamt fuer Verfassungsschutz ( <i>BfV</i> ) (C / V) Amt fur Nachrichtenwesen der Bundeswehr ( <i>ANBw</i> ) (M / I) Militaerischer Abschirmdienst ( <i>MAD</i> ) (M / V)	<b>POLEN</b> 	Agency for Protection of the State ( <i>UOP</i> ) (C / VI) Military Intelligence Service ( <i>WSI</i> ) (M / I)
<b>FRANKRIJK</b> 	Direction Générale de la Sécurité Extérieure ( <i>DGSE</i> ) (C / I) Direction du Renseignement Militaire ( <i>DRM</i> ) (M / I) Direction de la Surveillance du Territoire ( <i>DST</i> ) (M / V) Direction Centrale Renseignements Généraux ( <i>RG</i> ) (C / V) Direction de la Protection et de la Sécurité de la Défense ( <i>DSPD</i> ) (M / V)	<b>RUSLAND</b> 	Committee for State Security ( <i>KGB</i> ) (C / VI) Main Intelligence Directorate ( <i>GRU</i> ) (M / I) Foreign Intelligence Service ( <i>SVR</i> ) (C / I) Federal Security Service ( <i>FSB</i> ) (C / V)
<b>GRIEKENLAND</b> 	Greek Intelligence Service ( <i>KYP</i> ) (C / I)	<b>SPANJE</b> 	Centro Superior de Información de la Defensa ( <i>CESID</i> ) (M / I)
<b>GROOT BRITANNIE</b> 	Joint Intelligence Committee ( <i>JIC</i> ) (C / I) MI5 Security Service (C / I) MI6 Secret Intelligence Service ( <i>SIS</i> ) (C / I) Defence Intelligence Staff ( <i>DIS</i> ) (M / I) Government Communications Headquarters ( <i>GCHQ</i> ) (C / I) National Criminal Intelligence Service ( <i>NCIS</i> ) (C / VI)	<b>TSJECHIE</b> 	Military Counter Intelligence Service ( <i>VOZ</i> ) (M / V) Military Intelligence Service ( <i>RVZ</i> ) (M / I)
<b>HONGARIJE</b> 	Nemzetbiztonsági Hivatal ( <i>National Security Office</i> ) (C / V)	<b>TURKIJE</b> 	Milli Istihbarat Teskilati ( <i>MIT: National Intelligence Organization</i> ) (C / VI)
<b>ISRAEL</b> 	Institute for Intelligence and Special Tasks ( <i>MOSSAD</i> ) (C / VI) General Security Service ( <i>SHIN BET</i> ) (C / V) Military Intelligence ( <i>AMAN</i> ) (M / I) Bureau of Scientific Relations ( <i>LEKEM</i> ) (C / I)	<b>VERENIGDE STATEN</b> 	Central Intelligence Agency ( <i>CIA</i> ) (C / I) Federal Bureau of Investigation ( <i>FBI</i> ) (C / V) National Security Agency ( <i>NSA</i> ) (C / V) Defense Intelligence Agency ( <i>DIA</i> ) (M / I) Drugs Enforcement Administration ( <i>DEA</i> ) (C / VI)
		<b>ZWEDEN</b> 	Säkerhetspolisen (C / V) ( <i>Security Service of the National Police Board</i> )
		<b>ZWITSERLAND</b> 	Federal Ministry of Defence / Security Division (M / VI)

Legenda: C=Civiel, M=Militair / V=Veiligheid, I=Inlichtingen)

# Samenvattingen

## INLEIDING

- Het **editoriaal** gaat in op de achtergronden van dit nummer, de breedte van het domein en de invalshoeken.
- De Nederlandse diensten kennen sinds 1956 een 'Coördinator'. De huidige coördinator, **drs. Kuijken**, gaat in op zijn huidige en toekomstige taak.

## DE NATIONALE DIMENSIE

- **Dr. Engelen** beschrijft de geschiedenis van de Nederlandse inlichtingen- en veiligheidsdiensten in de twintigste eeuw.
- Generaal-majoor **Van Reijn** is directeur van de Militaire Inlichtingendienst. Hij informeert over taken, organisatie en werkwijze, nu en morgen.
- De heer **Van Hulst** is hoofd van de Binnenlandse Veiligheidsdienst. Hij gaat in op de taken, verantwoordelijkheden en bevoegdheden van zijn dienst.

## DE INTERNATIONALE DIMENSIE

- Generaal-majoor der mariniers (b.d.) **Van Kappen** beschrijft hoe de VN worstelt met het begrip 'inlichtingen'.
- De heer **Theunens** presenteert zijn gedachten over de rol van inlichtingen bij vredesoperaties. Er bestaat behoefte aan aanpassing.
- Generaal-majoor (b.d.) **Karssing** beschrijft de inlichtingenwereld binnen de NAVO.
- Ook de Europese Militaire Staf kan niet zonder inlichtingen. Brigade-generaal **Bokhoven** verduidelijkt deze Europese dimensie.

## RISICO'S EN DREIGINGEN

- **Drs. Akerboom** van de BVD gaat in op het fenomeen terrorisme en de dreiging die daarvan uitgaat.
- **Drs. Stienstra** gaat in op de mogelijke betekenis van biologische wapens.
- Luitenant-kolonel **drs. Van der Louw** gaat in op 'Information Operations', informatie als middel, doel en wapen.
- **Ir. Luijff** richt zich op de kwetsbaarheid van de moderne informatie-infrastructuur.

## DIVERSEN

- Geheimhouding en/of openheid? **Drs. De Jong** gebruikt Rusland om de dilemma's te verduidelijken.
- Overzicht inlichtingen- en veiligheidsdiensten NAVO-partners.

# Summaries

## INTRODUCTION

- The **editors** explain the reasons behind the issue; the scope and the different angles of observation.
- Since 1956 the Dutch Intelligence Community has a 'co-ordinator'. **Mr. Kuijken**, the present co-ordinator clarifies his tasks, now and tomorrow.

## THE NATIONAL PERSPECTIVE

- **Mr. Engelen** presents an overview of the history of Dutch Intelligence- and security-services in the twentieth century.
- Major-general (Royal Marines) **Van Reijn**, the Director of the Military Intelligence Service, informs about tasks, organisation and future developments.
- The Director of the National Security Service, **mr. Van Hulst** addresses tasks and organisation, now and in the future.

## THE INTERNATIONAL DIMENSION

- Major-general (ret.) **Van Kappen** shares his observations on the wrestling of the United Nations with 'intelligence'.
- **Mr. Theunens** presents his views on intelligence and peace (support) operations. There is a need for adjustment.
- Major-general (ret.) **Karssing** clarifies 'Intelligence and Security' within NATO and the way ahead.
- The European Military Staff needs 'Intelligence'. Brigade-general **Bokhoven** informs about the 'European dimension'.

## RISKS AND THREATS

- **Mr. Akerboom** from the Dutch National Security Service addresses terrorism at the dawn of the twenty-first century.
- The biological weapon is minuscule but might have an enormous impact. **Mr. Stienstra** presents the facts and figures.
- Information can be a means, a weapon and a target. **Ltcol Van der Louw** informs about 'Information Operations'.
- **Mr. Luijff** shares his thoughts on the vulnerabilities of our modern information-infrastructure and options to counter them.

## VARIOUS

- Secrecy and/or openness? **Mr. De Jong** uses the Russian experience to clarify the dilemmas.
- Intelligence- and security services NATO: an overview.