Magazine nationale veiligheid en crisisbeheersing

jaargang 1
nummer 3
maart 2008

Internationale conferentie nationale veiligheid

National Safety & Security

Responding to risks to citizens, communities and the nation

28 & 29 January 2008
The Netherlands

CabinetOffice

Minister Van Middelkoop over strategische verkenningen Defensie

Reacties op kanttekeningen basisvereisten crisismanagement

Opslag landbouwzaden Spitsbergen garantie voedselvoorziening

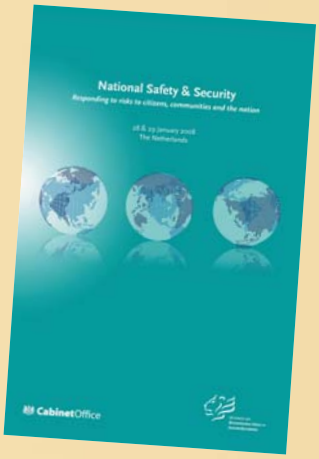
Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

Inhoud

Thema: Conferentie National Safety & Security 28-29 januari 2008

Het Magazine nationale veiligheid en crisisbeheersing is een maandelijkse uitgave van de directie Crisisbeheersing van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en verschijnt elf maal per jaar. Het blad informeert, signaleert en biedt een platform aan bestuurders en professionals over beleidsontwikkeling, innovatie, uitvoering en evaluatie ten aanzien van nationale veiligheid en crisisbeheersing. De verantwoordelijkheid voor de inhoud van de artikelen berust bij de auteurs.

Nationale veiligheid



Op 28 en 29 januari vond in Den Haag de conferentie *National Safety and Security: Responding to risks to citizens, communities and the nation* plaats. Meer dan honderd afgevaardigden van hoog niveau vanuit de hele wereld namen deel aan deze unieke bijeenkomst. Topambtenaren, managers van bedrijven en wetenschappers concludeerden dat de grootste uitdaging in de toekomst het ontwikkelen van een nauwere internationale samenwerking tussen alle spelers die deel uitmaken van de internationale veiligheidsgemeenschap - overheidsinstellingen, bedrijven en maatschappelijke organisaties – zal zijn. Dit is niet alleen het geval omdat we intern allemaal met dezelfde onderwerpen te maken hebben – dreigingsanalyses en het identificeren van de grootste risico's – maar ook omdat de dreigingen onderling samenhangen en niet stoppen bij grenzen. Bovendien zullen we in geval van een veiligheidsincident beter met elkaar moeten communiceren om kennis, expertise en hulpmiddelen te delen.

De conferentie verkende het thema vanuit drie perspectieven: het institutionele (hoe organiseren we nationale veiligheid), het analytische (welke methoden en instrumenten gebruiken we) en het sociaal-maatschappelijke (hoe verhogen we het risico-bewustzijn). Dit magazine is een weerslag van de discussies die tijdens de conferentie in de context van deze thema's plaatsvonden.

De conferentie is een belangrijke eerste stap in de richting van het samenbrengen van verschillende terreinen van veiligheid. We moeten er nu voor zorgen dat dit niet een eenmalig evenement was, maar dat deze bijeenkomst het begin vormt van een reis naar een intensievere samenwerking en echte vooruitgang met het oog op de dreigingen waar wij allen mee te maken hebben. Om dit te realiseren hebben de deelnemers afgesproken expertbijeenkomsten te organiseren op specifieke aspecten van nationale veiligheid en internationale instituten onderzoek uit te laten voeren. Zij spraken ook af om de waarde van het ontwikkelen van een informeel netwerk, waarvan de basis tijdens deze conferentie werd gelegd, te verkennen.

In zijn samenvatting stelde de dagvoorzitter, Professor Michael Clarke van het Royal United Services Institute for Defence and Security Studies, dat "de uitdaging van een crisis een combinatie van tijd, dreiging en verrassing is" en dat we daarom de plicht hebben om van elkaar te leren, onszelf voor te bereiden voor alle mogelijke gebeurtenissen en te erkennen dat we niet altijd alles kunnen voorkomen.

Het Verenigd Koninkrijk en Nederland zijn toegewijd aan het realiseren van vooruitgang van een netwerk, maar toekomstige initiatieven zullen moeten worden ingebracht en geleid door de bredere gemeenschap, zodat we werkelijk alles kunnen halen uit het internationale karakter van een dergelijk netwerk.

We hopen dat u met plezier deze speciale uitgave van het *Magazine nationale veiligheid en crisisbeheersing* zult lezen en erdoor geïnspireerd zult raken.

Bruce Mann,
Director Civil Contingencies Secretariat, UK Cabinet Office

Dick Schoof,
Directeur-generaal Veiligheid, ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Van *need to know* naar *need to share*

Openingstoespraak minister Ter Horst

Laat ik maar met de deur in huis vallen: het feit dat we hier zijn is niet zonder risico. We zitten hier weliswaar in het prachtige Kurhaus. Droog en ogenschijnlijk veilig. Maar u moet weten dat we ons hier ook bevinden op een plek die buiten de bescherming ligt tegen de zee. Ik wil geen onnodige onrust aanwakkeren. Ik wil alleen aangeven dat er reële dreigingen zijn, die vragen om onze aandacht. De Nederlandse regering is zich hiervan bewust. We zijn bezig om bedreigingen van de nationale veiligheid in kaart te brengen.

Laat ik eerst duidelijk maken wat we in Nederland onder nationale veiligheid verstaan. We spreken van nationale veiligheid wanneer onze vitale belangen in het geding zijn. We onderscheiden hierbij vijf categorieën: territoriale, economische, ecologische, fysieke en sociaal-politieke belangen. Aantasting van deze belangen kan leiden tot maatschappelijke ontwrichting. Twee zaken zijn daarbij duidelijk die ook voor u interessant zijn.

1. Nationale veiligheid is niet alleen een zaak van de overheid. Ook het bedrijfsleven en de burgers dragen verantwoordelijkheid. Er moet meer duidelijkheid op dit gebied komen. Ik kom daar zo op terug.
2. We zijn internationaal zó met elkaar verweven dat we elkaar nodig hebben. We kunnen nog veel beter profiteren van elkaars kennis en ervaring.

Ik weet zeker dat u al ervaringen aan het uitwisselen bent. Bijvoorbeeld over de overstromingen in Engeland, afgelopen zomer. Of de omvangrijke bosbranden in Griekenland. Sommige landen hebben het flink voor de kiezen gehad. We zijn geneigd vooral na te denken over wat geweest is en minder over wat zou kunnen gebeuren. Dat is ook lastig want de actualiteit haalt je vaak snel in. Sommige dreigingen lijken uit het niets op te duiken, zoals de SARS-uitbraak. Andere dreigingen zijn meer sluipend. We dachten bescherming te vinden in het gebruik van antibiotica, maar het dreigt onze vijand te worden. De toename van resistentie tegen antibiotica maakt ons helaas ook kwetsbaarder voor nieuwe ziektes. Nieuwe ziektes die door klimaatverandering of migratiestromen dichterbij komen. Knokkelkoorts bijvoorbeeld, is ineens weer een onderwerp waarover we in Nederland na moeten denken. Pandemieën zijn actuele nationale veiligheidsvraagstukken. Net zoals: digitale uitval, overstromingen, dierziekten en terrorisme. De rode draad is dat hierbij vitale belangen in het spel zijn.

De Nederlandse regering heeft april vorig jaar een nationale veiligheidsstrategie vastgesteld. In die strategie staan twee vragen centraal:

1. Wat komt er op ons af aan dreigingen en hoe erg is dat?
2. Wat is nodig om die dreigingen te voorkomen en wat is nodig als het toch gebeurt?

Er hoeft niet altijd een nationale ramp te gebeuren om het belang van zo'n strategie aan te tonen. Ik wil dan ook even stilstaan bij een gebeurtenis in Nederland op regionaal niveau.

Het gebeurde vlak voor Kerstmis. Een helikopter vloog tegen een hoogspanningsmast waarna die mast vervolgens in een grote rivier terechtkwam. Niet alleen werd de scheepvaart gestremd maar vanaf dat moment bleven 100.000 mensen gedurende 50 uur zonder stroom-

voorziening. Winkels moesten sluiten, het vee kon niet worden gemolken, rioleringen konden niet afvoeren met dreigende gevolgen voor het drinkwater, scholen moesten dicht. Dit incident bracht aan het licht dat twintig procent van de huishoudens in Nederland extra kwetsbaar is voor uitval. Dat heeft te maken met de manier waarop we ons energienet hebben aangelegd. Een verbetering kost circa 1 miljard. Het leidt tot complexe afwegingen: gaan we ons energienet aanpassen op basis van de risico-inschatting? Of vertellen we 20% van onze burgers dat ze een iets groter risico lopen op stroomuitval en dat we ze aanraden om een noodaggregaat aan te schaffen? Of zijn de noodaggregaten de verantwoordelijkheid van de energiesector?

Een soortgelijke vraag speelt op dit moment rondom het evacueren van burgers bij overstromingen. Kan de overheid bij een dijkdoorbraak en het onderlopen van een groot deel van Nederland, alle burgers tijdig evacueren? Als snelwegen vastlopen en de hulpdiensten mogelijk niet uit kunnen rukken door storm? Moeten we burgers niet duidelijk maken dat ze wellicht de eerste 24 uur voor zichzelf moeten zorgen? Dit voorbeeld raakt wat mij betreft twee belangrijke punten:

1. Hoe belangrijk het is om verantwoordelijkheden tussen burger, overheid en bedrijfsleven af te bakenen.
2. Hoe belangrijk het is dat we gefundeerde dreigingsanalyses en risico-inschattingen maken.

Ik kom daarmee op het punt van 'capability based planning'. Bij een goede dreigingsanalyse hoort ook de vraag: over welke capaciteit moet de overheid en het bedrijfsleven beschikken om met die dreiging om te kunnen gaan? Internationale bijstand kan daarbij een belangrijke rol spelen. Misschien kent u het rapport van de Franse minister Barnier hierover. Naar aanleiding van de bosbranden in Griekenland kwam Barnier in zijn rapport tot het voorstel om een Europese interventiemacht in te stellen. Dat klinkt mooi, maar wat voor soort interventiemacht zou dit moeten zijn, gezien de complexiteit van dreigingen? Het is volgens mij beter te focussen op de capaciteit die we als landen van elkaar kunnen gebruiken. Een mooi voorbeeld hiervan is het Urban Search en Rescue Team dat we in Nederland tot onze beschikking hebben en dat al vaker in het buitenland is ingezet. Ik zie niet veel in een centrale eenheid die staat te verstoffen als er niets gebeurt. Ik zie wel veel in goede afspraken tussen landen over wederzijdse ondersteuning.

Daarmee kom ik op de noodzaak tot samenwerking en de essentie van deze conferentie. We zijn ons er steeds meer van bewust dat het beschermen van de nationale veiligheid niet het domein is van één individueel land. Het is ook niet het domein van de publieke sector. Het gaat ons allen aan. We zijn onderling met elkaar verweven. Dit bleek alleen al uit de recente vogelgriepepidemie: op het gebied van kennisdeling en maatregelen hadden we elkaar nodig. Op dat punt is winst te behalen. We kunnen nog veel beter profiteren van elkaar. Dat geldt bijvoorbeeld voor publieke en private instellingen binnen een land, maar het geldt ook voor landen onderling. Wij allen zijn bezig met het inschatten van risico's.
De samenwerking zou een verschuiving moeten maken van *need to know* naar *need to share*. Op dit moment beperken we ons vaak tot het delen van het hoogstnoodzakelijke, en meestal op het moment na de ramp, maar het gebeurt nog te weinig in de preventieve fase. Dat is te verklaren. Veiligheidsorganisaties laten niet graag in hun keuken kijken. Datzelfde geldt voor de private sector. Door onderlinge concurrentie zijn energieleveranciers of telecombedrijven terughoudend in de openheid over kwetsbaarheden. Hun imago en marktpositie staat op het spel. Gelukkig dringt het besef steeds meer door dat we elkaar nodig hebben. Medewerkers van verschillende landen zoeken elkaar meer en meer op. Langzaam maar zeker ontstaat er een netwerk van kennis en ervaring. Maar daar kunnen we wellicht meer structuur aan geven, zonder het te formaliseren. Want het moet dicht bij de praktijk blijven. Vandaag biedt daar een goede gelegenheid voor.

Ik wil mijn waardering uitspreken voor de prettige manier waarop we deze bijeenkomst samen met onze partners vanuit het Verenigd Koninkrijk hebben voorbereid. Het is geen toeval dat Nederland dit samen met het Verenigd Koninkrijk heeft gedaan. Nederland heeft voor de eigen analyse van de nationale veiligheid veel gebruik gemaakt van de *all hazard* methode om risico's in kaart te brengen. Engeland heeft gebruik gemaakt van de Nederlandse methode om de strategie nationale veiligheid op te zetten. We hebben met andere woorden geprofiteerd van elkaars sterke kanten. Het zou mooi zijn als dit op bredere schaal zou kunnen. Ik roep dan ook op om vandaag concrete stappen te zetten. Laten we bijvoorbeeld komen tot een *community of best practices*. Het is een uitstekend idee waar je in de praktijk iets aan hebt.

Ik sluit af met de verwachting dat we aan het eind van de dag de verschuiving hebben ingezet van *need to know* naar *need to share*. Onze samenwerking heeft verdieping nodig. Mocht u gedurende de dag toch op een dood spoor komen, kijkt u dan even uit het raam naar de zee. Het ziet er mooi uit, maar we nemen een gecalculeerd risico, weet u nog. Laat deze plek u inspireren tot daadkracht.

Ik wens u veel succes.

mw. dr. G. ter Horst,
minister van Binnenlandse Zaken en Koninkrijksrelaties

Nationale veiligheid: een uitdaging voor internationale samenwerking?

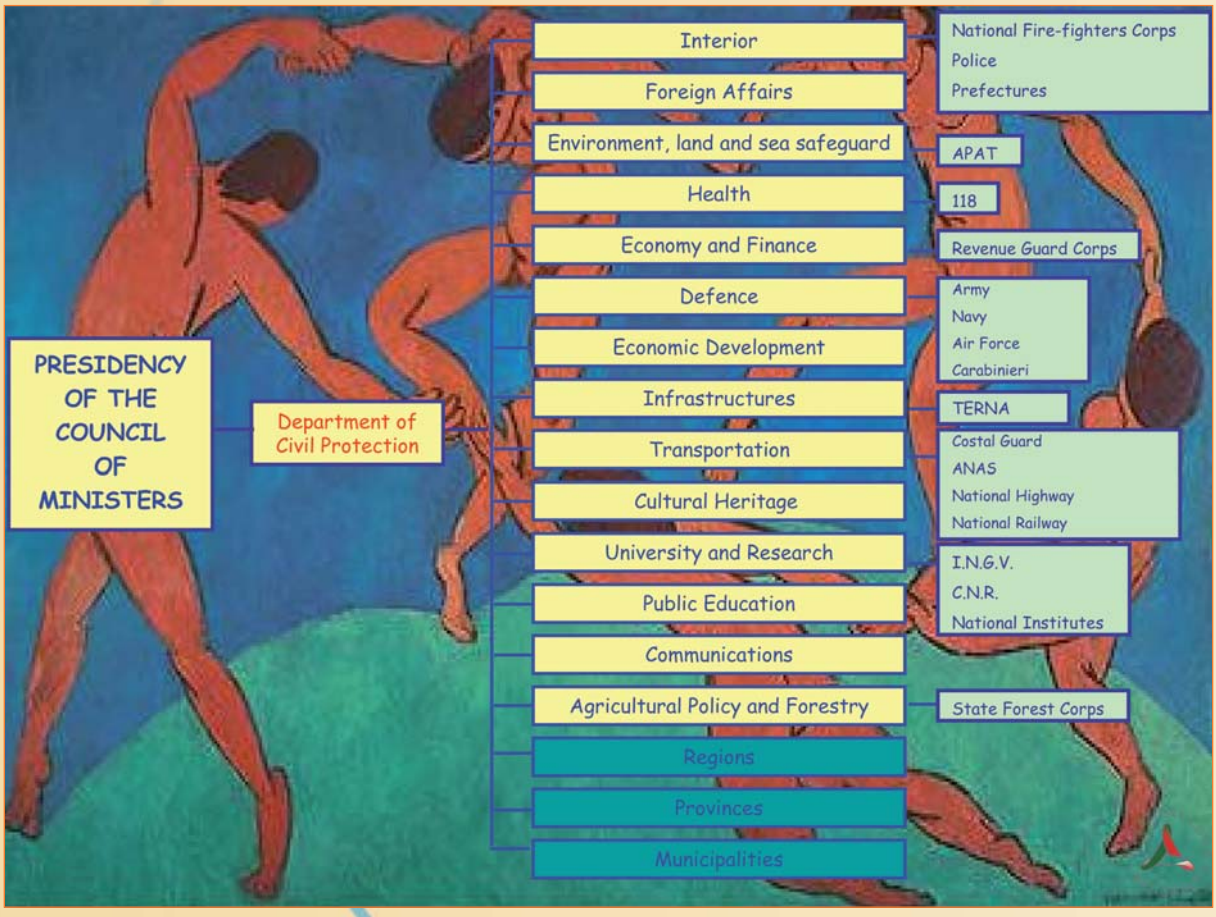
In deze bijdrage gaat directeur-generaal Civiele Bescherming Guido Bertolaso gaat in op de hedendaagse dreigingen en de besluitvorming en operationele structuur op nationaal niveau in Italië.

Waar het naar mijn mening werkelijk om draait – afgezien van de kans de handen op internationaal niveau ineen te slaan bij bijvoorbeeld pandemieën veroorzaakt door onbekende pathogene organismen, terroristische aanslagen of grootscheepse overstromingen en of we deze zogenaamde "traditionele" gevaren dan efficiënter en beter het hoofd zouden kunnen bieden – is de vraag hoe we onze krachten zouden kunnen bundelen om adequaat te kunnen reageren op de steeds hoger wordende eisen.

Daarom wil ik het hebben over manieren om samen te werken, want uitgaand van de recente geschiedenis staat een bevestigend antwoord wel vast. Als we bezien wat er na de Tweede Wereldoorlog gebeurde, kunnen we constateren dat er steeds meer werd samengewerkt in allerlei sectoren en met allerlei aanleidingen. Dat leidde tot de oprichting van de Europese Unie, zoals op ons continent, of de NAVO op militair gebied en zelfs de Verenigde Naties, als we er het Westen en vervolgens de hele wereld bij betrekken.

Ik wil hier echter benadrukken dat vooral de veelgehoorde kritiek in onze landen mij zorgen baart als het gaat om internationale samenwerking: de vermoeiende en trage besluitvorming en de discrepantie tussen de tijd voor verschillende noodscenario's om zich te ontvouwen en de tijd die nodig is om de middelen en wilskracht te mobiliseren voor ingrijpen.

Ik denk dat die kritiek gegrond is. Mijn ervaringen als hoofd van de civiele bescherming in Italië hebben mij ervan doordrongen dat de variabele "tijd" de kern is van het nieuwe samenwerkingsmodel dat we nodig hebben



om de nieuwe gevaren het hoofd te bieden. Tijd is een primair schaars middel in noodsituaties. Daarom moeten we leren de nieuwe gevaren te beheersen zonder belemmerd te worden door de organisatorische structuren waar we in het verleden ons heil in zochten.

Afgezien van de factor tijd als centraal element in onze discussie over veiligheid wil ik erop wijzen dat we het model van staten en internationale organisaties zoals dat eeuwenlang heeft bestaan, zullen moeten verlaten.
Ik wil het eerst hebben over dit organisatieprobleem.
Ik heb eens gezegd dat de moderne natiestaat ontstaan is als het beste organisatorische model voor een maatschappij als bescherming tegen de gevaren die het leven en de kwaliteit van het leven van haar inwoners bedreigen.

Voor de traditionele gevaren en mogelijke natuurrampen zijn er instanties: elk land beschikt wel over een brandweerorganisatie (Vigili del Fuoco, Fire Brigade, sapeurs-pompiers, Bomberos, etc.) en diverse overheidsinstanties die het grondgebied bewaken, variërend van autoriteiten die zich bezighouden met de waterhuishouding tot en met het observatorium voor de Vesuvius (de oudste Europese instantie die vulkanische activiteiten registreert).

We maken ons zorgen over het vermogen van organisaties (bijv. FAO, UHNCR, WHO, Unicef) adequaat te reageren op de nieuwe gevaren, want we hebben nu te maken met andere scenario's dan een paar jaar geleden. We moeten met name de volgende vier factoren in het oog houden:

- de steeds grotere afstand tussen de maatschappij en de gespecialiseerde instanties die zijn opgericht voor noodsituaties en gevaren;
- het feit dat we kwetsbaarder zijn geworden voor gevaren zoals wordt benadrukt door de publieke opinie;
- de enorme omvang van veel catastrofes ten gevolge van de nieuwe gevaren;
- de complexiteit van het beheersen van noodsituaties, zowel qua schade, slachtoffers en doden, als de gevolgen ervan voor de publieke opinie.

Deskundigen en onderzoekers schrijven deze intensere reacties op bedreigingen voor de veiligheid toe aan verschillende factoren. Ik wil er slechts een paar noemen:

- het, om budgettaire redenen, geleidelijk afbrokkelen van de beschermende sociale netwerken en het wijdverbreide gevoel van onveiligheid dat hierdoor ontstaat;
- de groeiende onzekerheid omtrent werk en de organisatie van de verschillende levensfasen;
- de nadruk in de media op nieuws op veiligheidsgebied, vanwege de grote aandacht die ze ermee krijgen;
- en ten slotte het toenemende tempo van economische en sociale veranderingen ten gevolge van de globalisering, die mensen vaak ervaren door de intensiteit van de immigratiestromen en de terugkeer van de "vreemdeling" die als een bedreiging wordt gezien.

Onlangs is duidelijk geworden dat de feitelijke of door de media gesignaleerde gevolgen van bepaalde catastrofes die in verband worden gebracht met "nieuwe gevaren" aanleiding zijn voor twijfel of onze traditionele interventiemiddelen nog adequaat zijn. Geen enkel land beschikt over een "op competenties gebaseerde" structuur met voldoende middelen om een orkaan als Katrina in alle opzichten zelfstandig het hoofd te kunnen bieden, laat staan de tsunami van 2004 die de kustplaatsen van zoveel landen aan de Indische Oceaan wegvaagde. Het ligt ook voor de hand dat geen enkel land kan bogen op een speciale structuur die de burgers tegen terroristische aanslagen kan beschermen. Dit soort catastrofes, zowel voorspelbare als onvoorspelbare, kan effectief worden aangepakt, mits het "op competenties gebaseerde model" wordt verlaten.

De "nieuwe gevaren" vormen in feite een nieuwe bedreiging die als veel gevaarlijker wordt ervaren dan andere:

- omdat de voorspelbaarheid van catastrofes klein is, een risico is namelijk onbekend, ofwel naar zijn aard, danwel vanwege de onvoorspelbaarheid;
- omdat rampen "buitenproportionele" gevolgen kunnen hebben ten opzichte van hetgeen we normaliter beheersen en aanvaarden, uitgaande van de mate waarin we voorbereid zijn;
- omdat ze grote opschudding in de media veroorzaken die leiden tot onbeheersbare emotionele reacties die op hun beurt sterke maatschappelijke reacties oproepen;
- omdat de respons op de bedreiging onhoudbare kosten met zich meebrengt, of een bepaald soort gedrag >>>

van burgers vereist, dat zij afwijzen of als onaanvaardbaar beschouwen omdat zij dan moeten afzien van eerder verworven rechten.

Voortredenerend op de kenmerken van deze “nieuwe gevaren” keren we terug naar de variabele “tijd" die ik eerder noemde, in de zin van “real time", dus de specifieke tijd van de ramp. De “tijd” waar het aan lijkt te ontbreken is in feite de “real time” waar we in Italië mee aan de slag zijn gegaan en opmerkelijke resultaten mee hebben geboekt bij het verbeteren van ons vermogen complexe gebeurtenissen het hoofd te bieden, ook wanneer ze plotsklaps of onaangekondigd plaatsvinden. Wij hebben geleerd de voor elke ramp specifieke “real time” te beheersen door het op “competenties gebaseerde" organisatiemodel te verlaten en te gaan experimenteren met een type overheidsorganisatie gebaseerd op “functies”.

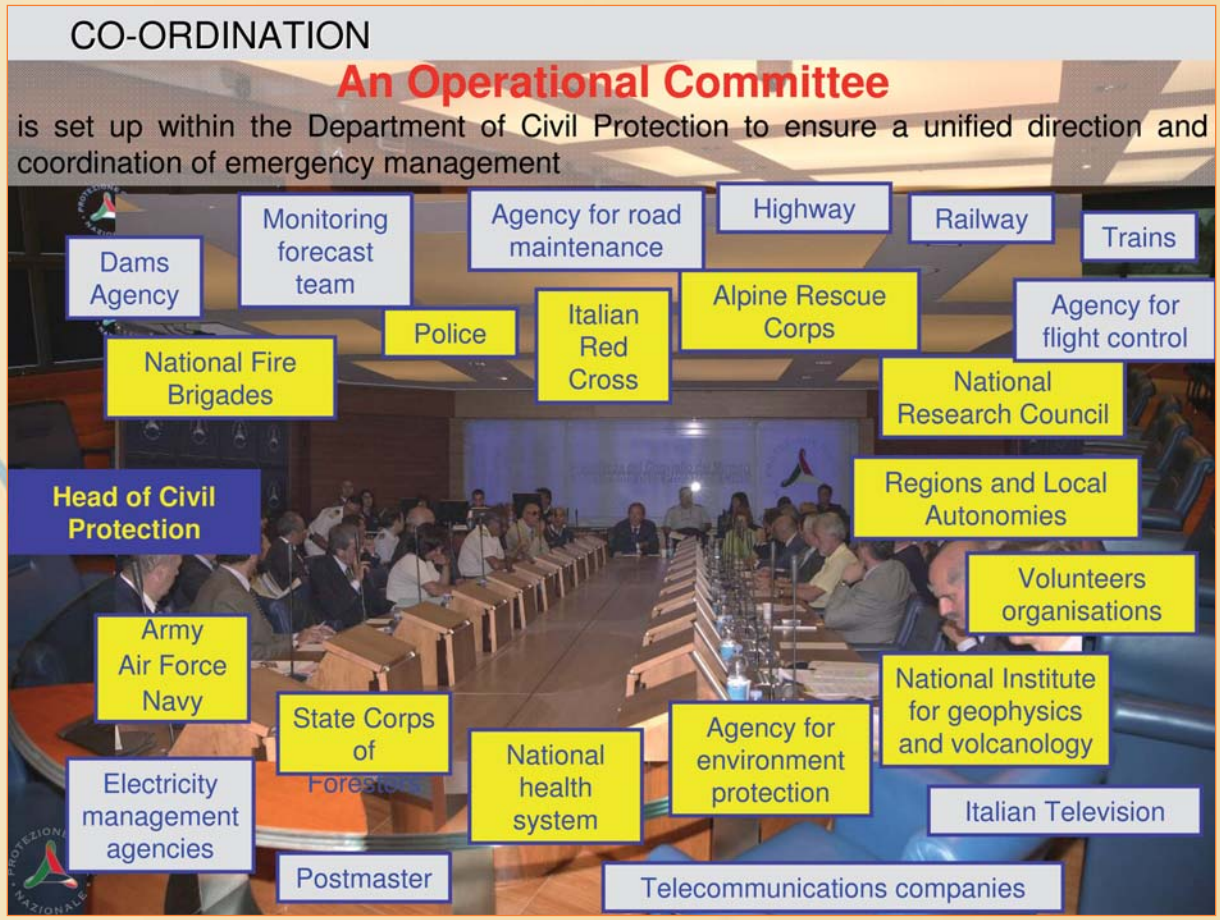
De geschiedenis van de civiele bescherming in Italië is interessant aangezien ons land een systeem heeft opgezet dat uitsluitend uitgaat van de tijd van de noodsituatie en van de gevaren, gevolgen en risico’s ervan.

Het systeem van de civiele bescherming is belast met de continue observatie van de risico's die in real time een gevaar voor de bevolking zouden kunnen vormen en heeft voorts tot taak waar dat mogelijk en nuttig is voorspellingen te doen, preventieve maatregelen te treffen en directe hulp te organiseren en noodmaatregelen te coördineren. Deze werkzaamheden worden verricht door een kleine groep mensen die direct onder de premier vallen. Dezelfde organisatiestructuur geldt op regionaal en lokaal niveau.

De afdeling civiele bescherming is een generale staf die beschikt over technische en wetenschappelijke functies zodat er te allen tijde informatie beschikbaar is voor de besluitvorming, maar beschikt niet over een eigen leger. De afdeling is echter wel bevoegd om de krachten te mobiliseren die nodig zijn om een ramp het hoofd te bieden en is in staat van geval tot geval specifieke taskforces in te stellen waarvoor alle elementen worden aangetrokken die geschikt zijn voor een bepaalde crisis en wel volgens de “functies" die nodig zijn om actie te ondernemen.
Het hoofd van deze “noodregering" kan alle bestuurlijke onderdelen die “functioneel” betrokken zijn bijeenroepen voor het besluitvormingsproces dat uitsluitend gericht is op de noodsituatie en het onmiddellijke optreden. De noodregering geeft orders aan de afdelingen, organen en structuren die deel uitmaken van de gewone overheid, waaronder de strijdkrachten en de politie. Ook vrijwilligersgroepen en organen voor de volksgezondheid alsmede gespecialiseerde bedrijven en deskundigen voor elk type gevaar kunnen worden gemobiliseerd. De mobilisatieprocedures zijn vastgelegd en vallen onder gemeenschappelijke procedures die iedereen kent: zodra zich een ramp voordoet wordt er dus geen tijd verspild met onderhandelingen, toelichtingen en het afbakenen van grenzen. Iedereen die verantwoordelijk is voor en betrokken is bij de besluitvorming weet wat hem of haar te doen staat en hoe er moet worden gehandeld in een noodsituatie.

Het bestaan en daadwerkelijk functioneren van een “noodregering” levert weliswaar aanzienlijke problemen op, maar stelt ons ook in staat:

- de tijd die nodig is voor verschillende soorten hulpverlening aan de bevolking tot een minimum te beperken;
- de interventietijd te bekorten;
- een systeem op te zetten dat weinig menselijke en economische hulpbronnen vergt in vergelijking met hetgeen het daadwerkelijk op de been kan brengen;
- territoriaal hetzelfde model op basis van “mobilisatie naar functie” van middelen toe te passen die normaliter voor andere taken zijn gereserveerd;
- op deze manier de grootst mogelijke veerkracht te bewerkstelligen;
- een snelle besluitvorming te waarborgen zonder uitsluiting van territoriale bestuurlijke eenheden en operationele procedures die inherent zijn aan noodsituaties;



- en bovendien hoeven we geen hiërarchie van risico's op grond van de verwachte ernst of interventieprioriteiten vast te stellen. Voor het civiele beschermingssysteem zijn alle noodsituaties gelijk, ongeacht de oorzaak.

Zo wordt een competentiestrijd tussen bestuurlijke eenheden bij ernstige en complexe situaties vermeden, mochten er op hetzelfde moment verschillende competenties aan bod komen; bovendien wordt onduidelijkheid voorkomen door ze als "functies" te behandelen die nodig zijn om het probleem te verhelpen.
Dankzij de besluitvorming en operationele structuur van de civiele bescherming, de zichtbare bescherming en de geboekte resultaten heeft Italië zijn burgers gerust kunnen stellen.

De weg van een op competenties gebaseerde organisatie naar een op functies georiënteerde structuur verloopt via een proces waarbij horizontale coördinatie (zoals de clusterstrategie van de VN of de MIC-procedures van Europa) achterwege zou moeten blijven. Deze pogingen hebben namelijk geen kans van slagen omdat ze de "gouvernementele" problemen niet verhelpen.
Ik ben ervan overtuigd dat experimenten met een op functies gebaseerd gouvernementeel systeem op Europees en mondiaal niveau snel zouden leiden tot meer efficiëntie en effectiviteit bij het beschermen van onze burgers tegen "nieuwe gevaren" en op internationale schaal betere interventiemethodes zouden bewerkstelligen voor situaties waarin de gevolgen van een catastrofe de capaciteiten van het getroffen land te boven gaan.
Het opzetten van een op functies gebaseerd internationaal systeem hoeft geen kostbare operatie te zijn, aangezien een snel gecoördineerd commandoniveau en snelle besluitvormingslijnen worden opgezet op basis van vooraf besproken procedures.
Het scenario dat ik zojuist heb geschetst brengt echter wel andere kosten met zich mee, namelijk culturele kosten.

Italië heeft deze keuze gemaakt na talloze tragedies van uiteenlopende aard en na dramatische tijden te hebben doorgemaakt die de natuur andere landen bespaard heeft, waar sommige gevaren volledig onbekend zijn. Te denken valt hierbij aan aardbevingen of vulkaanuitbarstingen.
In tegenstelling tot de traditionele gevaren stellen "nieuwe gevaren" al onze landen bloot aan gevaren en mogelijke catastrofes die hun weerga niet kennen. Ik hoop dat de ervaringen van mijn land – dat eerder dan andere werd geconfronteerd met rampen met uiteenlopende oorzaken – van nut kunnen zijn bij het vinden van nationale oplossingen en vormen van internationale samenwerking waarmee kan worden voldaan aan de behoefte van onze burgers aan veiligheid en bescherming die zij als een verworven recht beschouwen.

Guido Bertolaso,
Director-General, Department of Civil Protection, Prime Minister's Office

Veiligheid en het belang van proportionaliteit en samenwerking

Peter de Wit, president-directeur Shell Nederland

Voordat ik uitgebreid inga op de visie van Shell op veiligheid en beveiliging, wil ik even stilstaan bij de ideale locatie van deze conferentie. Het lokale openbaar vervoer functioneerde zoals het hoort, dus u was hier op tijd. Het was wellicht wat druk op de weg, maar mocht u echt stil hebben gestaan, dan was dat in elk geval niet vanwege brandstofschaarste. De verlichting is aan, de verwarming doet het, via computers en Black Berry's kunt u de gewenste informatie vinden en niemand van u zal zich afvragen of er hier tussen de middag wel iets te eten en te drinken zal zijn. Buiten buldert de zee, maar miljoenen mensen kunnen zich hier – een paar meter onder de zeespiegel achter een smalle duinenrij – veilig wijden aan de dagelijkse routine.

Zelden zal hier iemand ook maar een seconde bij stilstaan. Want het lijkt alsof dat allemaal vanzelf gaat. Schijn bedriegt echter. Je zou het kunnen vergelijken met het uurwerk van een klok dat met de grootste precisie in elkaar is gezet en verrassend accuraat de tijd aangeeft. Maar dan mag er beslist geen zandkorreltje tussen de radertjes komen. Die spreekwoordelijke korreltjes zand komen we echter overal tegen, soms omdat de natuur ons parten speelt en soms omdat ze met opzet zijn rondgestrooid door bepaalde individuen. Intussen worden er steeds meer beveiligings- en veiligheidsmensen ingezet om onze uurwerken vrij te houden van zandkorreltjes. En daar slagen ze heel wat beter in dan de meeste mensen denken: als je iets niet ziet, ben je geneigd te denken dat het niet bestaat óf dat het vanzelf gebeurt. Zoals eten op tafel, stroom uit het stopcontact en benzine bij het tankstation.

Maar in onze zeer gespecialiseerde wereld kunnen we ons de illusie dat dingen vanzelf gebeuren niet permitteren dankzij hun eenvoud maar vanwege een hoge mate van professionaliteit. Veiligheid heb ik al genoemd in dit verband en daar wil ik graag een aantal aspecten uitlichten. Ik zal stilstaan bij:

- de vitale infrastructuur en de beveiliging daarvan;
- de zekerheid van de olie- en gastoevoer naar Europa;
- de manier waarop Shell zijn veiligheidsbeleid georganiseerd heeft;
- de manieren waarop regeringen, handel en industrie hun veiligheidsinfrastructuur kunnen optimaliseren door beter samen te werken.

Vitale infrastructuur en beveiliging

Meestal loopt alles op rolletjes, maar dan gaat er ineens iets fout. Dan treedt er plots een storing op in iets dat vitale infrastructuur blijkt te zijn. Dat merkten we onlangs in Nederland toen er een helikopter tegen drie hoogspanningskabels boven een rivier vloog. Honderdduizend mensen moesten het 48 uur zonder elektriciteit stellen. Het was dan wel geen regelrechte ramp, maar wel heel problematisch én duur. Want wat bleek: de elektriciteitsvoorziening voor het getroffen gebied hing volledig af van die drie kabels hoog boven een rivier, die ook nog eens buiten haar oevers pleegt te treden in de winter. De lering die hieruit getrokken werd, is dat elk onderdeel van de vitale infrastructuur dus altijd in een lus moet worden aangelegd. Als de voordeur niet open kan, moet het mogelijk zijn de boodschappen gewoon via

de achterdeur naar binnen te brengen of desnoods via een raam boven. Dit bevordert in de eerste plaats de zekerheid van leveranties. Beheersystemen worden op die manier betrouwbaarder en bovendien worden zo de capaciteit en efficiency van de infrastructuur verbeterd.

Als potentiële terroristen weten dat vitale infrastructuur altijd dubbel of zelfs in drievoud aanwezig is, zullen zij hun oog daar minder snel op laten vallen bij het kiezen van mogelijke doelwitten. Het doel van terrorisme is per slot van rekening ontwrichting van de maatschappij om zo de politieke besluitvorming te beïnvloeden.

In Nederland is de NAM, een gasproducent onder beheer van Shell, aangewezen als “vitale onderneming”. Honderden werklocaties van de NAM zijn onderverdeeld in vier categorieën naar de ernst van de gevolgen voor de maatschappij, als ze uitgeschakeld zouden worden. De NCTb is nu proceseigenaar van al deze systemen en beheert bij wijze van proef het NAVI, het Nationaal Adviescentrum Vitale Infrastructuur voor het hele land. Dit centrum levert advies en expertise omtrent de beste praktijken afkomstig van overheidsorganen en andere relevante terreinen. Als eigenaar en beheerder van heel wat vitale infrastructuur onderhoudt Shell intensieve contacten met het NAVI. Dit is de tweede rechtstreekse lijn tussen Shell en de overheidsorganen die verantwoordelijk zijn voor de veiligheid. De andere lijn bestaat vanwege de raffinage- en chemische activiteiten van Shell die deel uitmaken van het Nationale Alerteringssysteem. Via dit systeem worden dreigingsniveaus vastgesteld waar de aangesloten ondernemingen hun interne beveiliging op kunnen afstemmen.

Zekerheid olie- en gastoevoer Europa

Qua volume is olie onze grootste energiebron, die bovendien vaak van grote invloed is op de gasprijs. Olie vormt een uitzondering op de regel van de alomtegenwoordige just-in-time logistiek zonder voorraden die je overal aantreft in de huidige economie.

Na de oliecrisis van 1973 hebben een aantal OESO-lidstaten het IEA (Internationaal Energie Agentschap) opgezet. De belangrijkste taak van dit coördinerende agentschap in Parijs is het veiligstellen en toewijzen van olievoorraden in tijden van crisis. De aangesloten landen (26 in totaal) hebben het volgende afgesproken:

- De landen houden voorraden aan van ten minste 90 dagen aan netto olie-importen. Deze reserves behoeven zich niet noodzakelijkerwijs in de landen zelf te bevinden. Veel West-Europese landen hebben hun olievoorraden bijvoorbeeld in de ARA-regio (Amsterdam, Rotterdam en Antwerpen).
- Bij problemen nemen de landen passende maatregelen, zoals beperking van het verbruik, overschakelen naar andere brandstoffen en indien mogelijk verhoging van de energieproductie in eigen land.
- Indien de olieaanvoer ernstig verstoord raakt (daarvan is sprake bij een krimping met ten minste 7 procent) treedt er onder leiding van het IEA een toewijzingssysteem in werking.
  Dan wordt er olie uit de strategische reserves en voorraden toegewezen en verdeeld over de lidstaten.

Het systeem trad bijvoorbeeld in werking in 1990 en 1991 na de inval van Irak in Koeweit. Bij deze invasie en de Amerikaanse interventies gingen per dag 4,3 miljoen vaten aan olieproductie verloren, terwijl de mondiale productie op dat moment 65 miljoen vaten per dag bedroeg. Om het even in een perspectief te plaatsen: momenteel worden er per dag 87 miljoen vaten verbruikt en volgens het IEA kan dat tegen 2030 opgelopen zijn tot ergens tussen de 102 en 116 miljoen vaten.

Twee jaar geleden werd het systeem in beperkte mate ingeschakeld om de gevolgen van orkaan Katrina in de Golf van Mexico op te vangen. Toen werd een flinke hoeveelheid van de Nederlandse en Britse oliereserves overgebracht naar de Verenigde Staten waar verschillende productieplatforms en raffinaderijen uitgeschakeld waren. Strategische olievoorraden worden alleen ingezet om dreigende tekorten op te vangen, dus niet om in te grijpen bij prijsstijgingen op de markt.

’s Werelds grootste strategische olievoorraad is van de Verenigde Staten en bedraagt momenteel 700 miljoen vaten ruwe olie, wat ongeveer neerkomt op 55 dagen aan olie-importen. Aan het eind van 2007 tekende president Bush een wet om de strategische oliereserve vóór 2027 uit te breiden tot 1,5 miljard vaten. China is intussen zijn eigen veiligheidsbuffer gaan opzetten.

De strategische oliereserves hebben tot dusver goed gefunctioneerd, hoewel ze hoogstzelden worden aangesproken, weerhouden ze landen ervan olie voor politieke doeleinden te gebruiken. In theorie hebben >>>

de olie-exporterende landen, gezamenlijk of individueel, de gelegenheid olie als drukmiddel te gebruiken en dat is in het verleden ook wel gebeurd. De mondiale productie-capaciteit is per slot van rekening maar iets groter dan het mondiale verbruik. Wanneer een van de grotere exporterende landen zou besluiten de leveranties om welke reden dan ook op te schorten, is er elders maar weinig capaciteit over om dat op te vangen. Dit risico moet echter niet overdreven worden. Olie-exporterende landen kunnen hun economieën niet draaiende houden zonder olie-inkomsten en zouden al snel geconfronteerd worden met sociale onrust. Maar vanwege deze geringe overcapaciteit vormen terroristische aanslagen op grote olieproducenten of havenfaciliteiten en scheepvaartroutes dus een ernstige bedreiging.

Ter illustratie noem ik een paar fysieke knelpunten. Dagelijks worden er 13,4 miljoen vaten ruwe olie vervoerd via de Straat van Hormuz en 12 miljoen vaten via de Straat Malakka. Het IEA verwacht dat in 2030 30 procent van het totale mondiale olieverbruik via de Straat van Hormuz zijn weg naar de rest van de wereld zal vinden, dus bijna tweemaal zoveel als vandaag. Tijdens de tanker-oorlog van 1984 tot 1987 in de Perzische Golf daalden de olietransporten met 25 procent, maar toen was er nog voldoende reserveproductiecapaciteit in de rest van de wereld. Nu bevindt bijna alle reservecapaciteit zich bij de Straat van Hormuz.

Dan is er aardgas dat vooral wordt vervoerd via pijp-leidingen. Dat is veilig, maar weinig flexibel en zoals we hebben gemerkt op veel plaatsen bijna onmogelijk fysiek te beschermen. Pijpleidingen verbinden leverancier en klant direct met elkaar. LNG, *liquefied natural gas* oftewel vloeibaar gas, biedt een interessant alternatief, want dat kan per schip vervoerd worden; dat is weliswaar ook kwetsbaar, maar biedt meer mogelijkheden voor beveiliging. Het aantal leveranciers is momenteel nog beperkt, maar de markt groeit snel. Met name de Europese importen van aardgas blijven flink groeien. Volgens het IEA zal de jaarlijkse invoer stijgen van de huidige 235 miljard kubieke meter tot 520 miljard in 2030. Uiteindelijk zal de grootste veiligheid wat betreft de gasaanvoer te winnen zijn door spreiding van de toelevering. Dit wordt mogelijk door pijpleidingen, zoals het Noordstroomproject dat binnenkort zal worden aangelegd van Rusland door de Baltische zee, en veel terminals in Europa voor de invoer van LNG.

Het zal voor zich spreken dat al deze vitale infrastructuur voor de energievoorziening beschermd moet worden. Daarom wil ik nog stilstaan bij een andere dimensie van veiligheid: de bescherming van voorzieningen zelf. Omdat Shell overal ter wereld actief is, beschikken we over kennis uit de eerste hand van de uiteenlopende benaderingswijzen die overheidsinstanties hanteren. We zien in feite twee verschillende strategieën voor de beveiliging van fysieke installaties, die worden bepaald ofwel:

- door het risico ofwel;
- door de gevolgen.

De Europese benadering gaat uit van mogelijke gevaren en wordt dus gedicteerd door het risico. Dit systeem verschaft adequate antwoorden na een analyse van de gevaren. De risiconiveaus worden onderverdeeld in fasen en de eigenaren van vitale infrastructuur stemmen hun beveiligingssystemen en –maatregelen daar op af. Het Europese model biedt de grootste kans op een proportionele reactie. In de Verenigde Staten is het meer de gewoonte de maximaal mogelijke gevolgen in kaart te brengen, bijvoorbeeld van een grootschalige aanval op installaties. Op basis van deze aanpak die meer op de gevolgen gericht is, worden installaties, gebouwen en systemen extra beveiligd. Dit betekent in de praktijk dat er grote sommen geld worden geïnvesteerd in het versterken van complexen zodat ze bestand zijn tegen eventualiteiten. Daar wordt dus voortdurend een hoog beveiligingsniveau gehandhaafd, ook wanneer het dreigingsniveau laag is. Het is misschien wat zwart-wit gesteld, maar illustreert wel de verschillen qua mentaliteit en wereldbeeld. Europeanen concluderen altijd snel dat de Amerikaanse veiligheidsmaatregelen overdreven zijn en de Amerikanen vinden dat de Europeanen naïef zijn en dingen te weinig serieus nemen. (Gek genoeg blijkt het tegenovergestelde wanneer het gaat om de bescherming van de kust.) Proportionaliteit is dus geboden. Het middel, de beveiliging van de maatschappij, mag qua gevolgen natuurlijk niet erger zijn dan de kwaal, dus de gevaren waarvoor het bedoeld is.

Hoe heeft Shell zijn beveiliging georganiseerd?

Wij hanteren een “All Hazards Approach” en zijn dus voorbereid op elk denkbaar incident, met welke aard of oorzaak dan ook. Dit betreft zowel veiligheid (HSE –

Health Safety & Environment) als beveiliging, en ook "*acts of God*" dus extreme weersomstandigheden, aardbevingen en overstromingen. Naar aanleiding van 11 september en de nasleep ervan heeft Shell zijn Security organisatie op groepsniveau georganiseerd, uitgebreid en geprofessionaliseerd en verantwoordelijk gemaakt voor de beveiliging van fysieke activa en mensen.

De afdeling Corporate Affairs Security (CAS) is hiervoor verantwoordelijk op groepsniveau. De CAS is een wereldwijd netwerk van beveiligingsprofessionals die deel uitmaken van de afzonderlijke bedrijfsonderdelen en onder leiding staan van een kerngroep van specialisten op het hoofdkantoor van Shell in Den Haag. Daarnaast hebben we binnen de financiële poot een aparte afdeling Business Integrity. Deze afdeling is verantwoordelijk voor de uitvoering van interne financiële forensische analyses.

Ook heeft Shell een eigen, aparte afdeling voor IT Security die tot taak heeft de kans op cybercriminaliteit te minimaliseren en de alertheid erop te vergroten. De CAS is daarmee primair verantwoordelijk voor het identificeren van risico's voor personeel en installaties.
De operationele procedures van de CAS zijn opgenomen in handboeken die zijn gebaseerd op de beveiligingsnormen van de groep. Hierin staan ook de vijf dreigingsniveaus die we binnen de onderneming hanteren en die variëren van "incidenteel/onwaarschijnlijk" tot "extreem". Onze groepsbeveiligingsnormen schrijven voor dat veiligheidsrisico's met regelmatige tussenpozen moeten worden geïdentificeerd en beoordeeld. Dat geldt ook voor de maatregelen die bedoeld zijn om deze risico's te beheersen en de gevolgen ervan tot een minimum te beperken. Deze beveiligingsprocessen en -procedures hebben hun waarde vlak voor kerst 2006 bewezen. Na een aantal ontvoeringen en bomaanslagen werd besloten de gezinnen van medewerkers uit Nigeria te repatriëren. Drie dagen later landden er in Amsterdam en Londen drie vliegtuigen met deze gezinsleden aan boord – een perfect uitgevoerde noodoperatie.
Veiligheidsproblemen kunnen soms enorm zijn qua omvang en complexiteit. Neem nu het Shellproject Pearl in Qatar waar aardgas zal worden omgezet in hoogwaardige middeldestillaten. Op het hoogtepunt van de bouwwerkzaamheden zullen er 40.000 mensen aan het werk zijn. Medio 2008 zullen er in de bouw in en rond Ras Laffan Industrial City en in andere gasprojecten ongeveer 120.000 mensen aan het werk zijn – en dat in een land met hooguit 900.000 inwoners.
Dit trekt een zware wissel op de nationale veiligheidskrachten van Qatar en legt veel verantwoordelijkheid bij de ondernemingen om de orde in de kampen op een humane manier te handhaven met voldoende oog voor mensenrechten en politieke rivaliteit.

Samenwerking overheid en bedrijfsleven

De nationale Security Manager van Shell Nederland is het directe aanspreekpunt voor overheidsorganisaties zoals de AIVD, NAVI, de rijksoverheid en de NCTb. In april 2005 sloot de sector olie en chemie zich aan bij het nationale alerteringssysteem, dat beheerd en gecontroleerd wordt door de NCTb. Indien de NCTb besluit het dreigingsniveau voor deze sector te verhogen wordt onze Security Manager hiervan op de hoogte gesteld en zet hij een aantal maatregelen in gang.
De oprichting van de NCTb in Nederland is een grote stap voorwaarts gebleken. De NCTb is ons directe aanspreekpunt bij bedreigingen en daarmee ook voor het intensiveren van de beveiliging van onze vitale infrastructuur in Nederland. Het NAVI zal zich hopelijk op een soortgelijke manier ontpoppen.
Als commerciële onderneming hopen we dat de autoriteiten erin slagen drie zaken te handhaven:

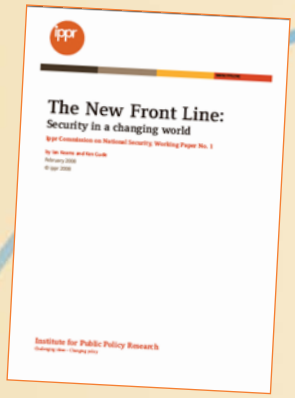
- hoogwaardige dreigingsanalyses (inlichtingen);
- open en snelle communicatie;
- een snelle en duidelijke reactie op elk incident.

We beseffen allemaal dat we altijd kwetsbaar zullen zijn vanwege de openheid die onlosmakelijk verbonden is met een democratische maatschappij. Maar 'democracy is not for the faint-hearted', dus we mogen geen slappe knieën krijgen. Daarom moeten we ondanks onze kwetsbaarheid de tegenwoordigheid van geest hebben om diegenen te weerstaan die onze waarden bedreigen. Samen kunnen we heel veel bereiken om de risico's te minimaliseren door onze gezamenlijke beveiligingsinspanningen verder te professionaliseren.

Wij van Shell onderkennen onze verantwoordelijkheden en zullen ernaar handelen.

Peter de Wit,
president-directeur van Shell Nederland

Nieuwe uitdagingen voor het Verenigd Koninkrijk op veiligheidsgebied [1]



De mondiale veiligheidssituatie is de afgelopen twintig jaar drastisch veranderd door ingrijpende gebeurtenissen als het einde van de Koude Oorlog en de aanslagen van 11 september. Dit alles heeft geleid tot nieuwe vraagstukken, actoren en risico's met verstrekkende gevolgen voor het veiligheidsbeleid van het Verenigd Koninkrijk (VK).

In de nieuwe situatie draait het om de wetenschap dat de conventionele opvattingen gebaseerd op een enkel front tot het verleden behoren: we hebben nu te maken met allerlei fronten die een heel scala aan veiligheidsvraagstukken betreffen. De reikwijdte en aard van de huidige veiligheidsrisico's omvatten weliswaar nog steeds de gebruikelijke zorg om terrorisme en de militaire verdediging van ons grondgebied maar gaan inmiddels veel verder dan dat. Overduidelijk is dat, willen we de risico's en gevaren waar het VK vandaag de dag mee geconfronteerd wordt effectief het hoofd kunnen bieden, we ons opnieuw zullen moeten bezinnen op de vraag wat het front in de strijd om de veiligheid is en ons antwoord daarop dienovereenkomstig aanpassen.

In dit artikel geven we een overzicht van de belangrijkste factoren voor de beveiliging van vandaag aan de hand van vijf hoofdthema's waarvan wij vinden dat ze tezamen een nuttig kader vormen voor het denken over de integrale veiligheidssituatie van nu. Het betreft:

- globalisering en het ontstaan van nieuwe machtscentra;
- armoede en falende staten;
- klimaatverandering;
- de groei van de politieke islam;
- sociaaleconomische kwetsbaarheid.

We gaan ook kort in op de gevolgen van de veranderingen op veiligheidsgebied voor het formuleren van het VK-beleid en pleiten voor een aanpak gekenmerkt door samenwerking en een holistische benadering. Tot slot staan we stil bij een aantal belangrijke factoren die aan de orde moeten komen bij het formuleren van een nieuwe veiligheidsstrategie voor het VK.

Het veranderde strategische landschap

Globalisering en het ontstaan van nieuwe machtscentra

Een belangrijk gegeven voor de huidige veiligheidssituatie is het ontstaan van nieuwe machtscentra. Deze verschuivingen komen hoofdzakelijk voort uit de globalisering en spelen zich af op een aantal niveaus.

Ten eerste is er sprake van een relatieve versnippering van de macht binnen en tussen staten. Dit blijkt duidelijk uit de verschuiving van de macht van de landen langs de Atlantische Oceaan naar Azië en de landen in de Stille Oceaan en wordt vooral geïllustreerd door de opkomst van China en India. Dit zijn belangrijke veranderingen in het geopolitieke landschap en kan erop wijzen dat de grote mogendheden hun strijd niet, zoals in de twintigste eeuw, op het Europese toneel voeren maar dat deze verschuift naar het mondiale podium. Andere drijvende krachten achter de versnippering van de macht tussen de staten zijn de opkomst van een nieuwe groep staten en regio's die als energieleveranciers in potentie grote invloed kunnen uitoefenen en de verspreiding van kernwapentechnologie naar nieuwe staten, hetgeen nieuwe regionale conflicten om de macht kan veroorzaken.

Ten tweede zijn we getuige van de verschuiving van de macht naar niet-statelijke actoren, zoals terroristische groeperingen, grensoverschrijdende criminele organisaties en transnationale politieke bewegingen. Dergelijke groeperingen vormen een blijvende structurele bedreiging voor het VK, aangezien ze er niet alleen in slagen bepaalde statelijke machtsattributen te verwerven, maar ook het karakter van sommige staten weten te veranderen en zelfs

[1] *Dit artikel is gebaseerd op een langer document, getiteld "The New Front Line: Security in a changing world" door Ian Kearns en Ken Gude (IPPR). Dit is het eerste werkdocument dat aan de Commission on National Security in the 21st Century van de IPPR is voorgelegd. Voor het volledige document en nadere gegevens over de werkzaamheden van deze commissie zie www.ippr.org/security.*

de legitimiteit van staten weten te ondermijnen op een wijze die vragen doet rijzen bij de gebruikelijke opvattingen over machtspolitiek.

Een derde dimensie van de verschuivingen in de macht heeft te maken met de toenemende onderlinge afhankelijkheid van staten, waardoor de veiligheid binnen staten steeds vaker bepaald wordt door hetgeen zich afspeelt in andere staten. Door de globaliserende economie worden staten steeds gevoeliger voor veranderingen buiten hun grenzen. Voor het VK leidt een aantal internationale ontwikkelingen zoals het toegenomen grensoverschrijdende verkeer van personen en goederen en de groei van de internationale georganiseerde misdaad tot grotere onveiligheid op zijn grondgebied.

Armoede en falende staten

De tweede drijvende factor achter de veranderingen is de zogenaamde "veiligheids- en ontwikkelingsnexus", waar mondiale armoede, ongelijkheid, gewelddadige conflicten, falende staten en internationaal terrorisme elkaar treffen met mogelijk catastrofale gevolgen. Hoewel de verbanden tussen armoede en gewapende conflicten complex zijn en geenszins direct, is armoede een belangrijke verklaring voor gewapende conflicten, vooral in combinatie met toenemende ongelijkheid binnen en tussen groepen. Aangezien conflicten vaak een van de belangrijkste oorzaken voor armoede en onderontwikkeling vormen, lopen arme staten bovendien een verhoogd risico te vervallen in elkaar versterkende cycli van onderontwikkeling, conflicten, fragiliteit en zelfs ineenstorting. Falende staten zijn al humanitaire tragedies op zich, maar kunnen uitgroeien tot een belangrijke oorzaak voor regionale instabiliteit. Deze gebieden met een falende overheid kunnen een directe bedreiging vormen voor onze veiligheid, aangezien ze grote aantrekkingskracht uitoefenen op terroristische groeperingen en internationale criminele organisaties die het op ons gemunt kunnen hebben.

Klimaatverandering en schaarse middelen

Een derde factor achter de nieuwe veiligheidssituatie die onlangs op de mondiale politieke agenda opdook heeft te maken met de klimaatverandering. Voor sommige staten als Bangladesh en de eilandstaten in de Stille Oceaan zal de klimaatverandering spoedig de grootste bedreiging zijn voor hun veiligheid en bevolking. Maar ook elders zullen de gevolgen van de opwarming op de lange termijn bestaan uit grote verliezen van grond door de stijgende zeespiegel, ernstige tekorten aan water en voedsel en massale volksverhuizingen, aldus het International Panel on Climate Change (IPCC) recentelijk. Dit kan de huidige problemen op de mondiale veiligheidsagenda verder verergeren en nieuwe spanningen veroorzaken.

Ideologische conflicten: de uitdagingen van de politieke islam

Een vierde belangrijke factor in de huidige veiligheidssituatie is de groei van gewelddadige islamitische groeperingen, die zowel een directe bedreiging voor de openbare orde als een politieke bedreiging voor westerse liberale democratieën op de lange termijn vormen.
De moderne islam kan beter worden beschouwd als een politieke beweging die een bepaalde interpretatie van religie hanteert en niet zozeer als een fundamentalistische religieuze stroming die af en toe politiek bedrijft.
Door een combinatie van mondiale communicatie en de toenemende migratie van volken is de politieke islam erin geslaagd zijn greep buiten de landen met een moslimmeerderheid uit te breiden naar westerse liberale democratieën. Zoals gebleken bij de bomaanslagen in Londen in 2005 vormt de radicalisering onder moslims binnen en buiten het VK door gewelddadige islamitische groeperingen een belangrijke bedreiging voor de veiligheid van het VK. Ondanks de ernst van de dreiging die uitgaat van de islam ontbreekt het beleidsmakers van het VK nog altijd aan inzicht in de complexe oorzaken voor gewelddadig islamisme en radicalisering. Het ziet er dus naar uit dat er traag vooruitgang zal worden geboekt en dat de dreiging van het islamisme voorlopig een bepalende factor zal blijven voor de nationale en internationale veiligheidsagenda.

Sociaaleconomische veerkracht

Als vijfde factor achter de veranderingen beschouwen we de sociaaleconomische veerkracht. Het afgelopen >>>

decennium hebben Britse bedrijven hun operaties steeds verder afgeslankt, zijn ze "just-in-time" gaan produceren en hebben ze overtollig personeel afgestoten en hun voorraden tot een minimum teruggebracht. Dat vergt natuurlijk veel van de beveiliging en betrouwbaarheid van de ondersteunende infrastructuur zoals energie, communicatie en transport. De infrastructuur van het VK is echter steeds kwetsbaarder geworden voor storingen, vooral vanwege de onderlinge afhankelijkheid van de onderdelen ervan. Deze interdependentie maakt de infrastructuur gevoelig voor een soort domino-effect waarbij de uitval van een belangrijke sector van de infrastructuur – hetzij ten gevolge van een aanslag hetzij door een natuurramp – kan leiden tot de uitval van andere sectoren, met alle gevolgen van dien.

Het nieuwe front: afbakenen van het primaat van veiligheidsbeleid

De bovengenoemde veranderingen nopen duidelijk tot een omslag in het denken over veiligheid. De traditionele opvattingen over nationaal veiligheidsbeleid die gebaseerd zijn op het primaat van staten, de concurrentie tussen staten en militaire kwesties blijven in veel opzichten relevant, maar volstaan niet om de complexiteit van de huidige veiligheidssituatie adequaat te ondervangen. Het front in de strijd om de veiligheid heeft zich verplaatst en ligt mondiaal gezien thans in fragiele staten als Afghanistan waar Britse troepen momenteel gestationeerd zijn en in de internationale strijd tegen de klimaatverandering. Maar het ligt ook op lokaal niveau, binnen onze gemeenschappen, waar we de radicalisering en het extremisme aanpakken. Kortom: we hebben al lang niet meer te maken met één front, maar met vele, variërend van militaire tot milieu- en economische fronten.

We dienen een nieuwe nationale veiligheidsstrategie daarom in een ruimere context te plaatsen waarbij meer factoren en actoren in aanmerking worden genomen en op meerdere niveaus analyses worden gemaakt.

Samenwerking en veiligheid: een nieuwe aanpak

Willen we onze overheidsstructuren met succes verbeteren en uitbreiden naar dit nieuwe veiligheidsgebied, dan zijn samenwerking en een gecoördineerde aanpak, waarbij een breder scala aan beleidsinstrumenten en actoren kan worden ingezet, onontbeerlijk.

De voornaamste uitgangspunten voor samenwerking op veiligheidsgebied zijn:

- *Het begrip "geïntegreerde macht" aanvaarden*. Dit vereist toepassing van een ruimer scala aan beleidsinstrumenten om oplossingen op maat te creëren voor veiligheidskwesties, gebruik makend van zowel "harde", dus militaire en andere dwangmiddelen, als "zachte" sociale en economische instrumenten, echter zonder tussen een van beide categorieën te moeten kiezen.
- *Samenwerkingsverbanden met derden aangaan*. Dit betreft de kern van deze benadering en is relevant voor samenwerking op het multilaterale en regionale niveau maar ook op nationaal niveau tussen verschillende actoren binnen dezelfde staat.
- *Draagvlak creëren*. Voor zinvolle samenwerking zijn gemeenschappelijke doelen nodig die worden gedragen door alle actoren en dit kan alleen worden bewerkstelligd als er een breed politiek draagvlak is in de besluitvormingsprocessen. Bij onvoldoende politiek draagvlak lopen we het risico potentiële partners in internationale en nationale kringen van ons te vervreemden, waardoor ons vermogen de veiligheid te garanderen uitgehold wordt.
- *Transparantere beleidsvorming*. Draagvlak wordt alleen gecreëerd als alle actoren merken dat de beleidsvorming op veiligheidsgebied open en transparant verloopt. De overheid moet daarom zoeken naar mogelijkheden waar dat op een veilige manier kan.
- *Openstaan voor institutionele hervormingen*. De nieuwe veiligheidssituatie en de noodzaak beleidsinstrumenten te integreren vergen waarschijnlijk een wezenlijke institutionele hervorming op een aantal overheidsniveaus. Bestaande institutionele grenzen mogen deze innovatie niet in de weg staan.

Belangrijkste kwesties en conclusies

De voorgaande analyse heeft veel implicaties voor de beleidsvorming in het VK. De veiligheidssituatie is de afgelopen jaren drastisch veranderd en de beleidsmakers in het VK zullen alles in het werk moeten stellen om hun werk af te stemmen op het snelle tempo van die veranderingen. Indachtig de aankondiging van de Britse regering dat zij binnenkort een officiële nationale beveiligingsstrategie voor het Verenigd Koninkrijk bekend zal maken, besluiten we dit artikel met een aantal kwesties die naar onze mening dringend aandacht behoeven:

- Hoe kunnen we strategische *internationale instellingen* het best hervormen om te waarborgen dat ze beantwoorden aan de realiteit van de internationale orde en samenwerking op veiligheidsgebied bevorderen?
- Wat kunnen we doen om een *op regels gebaseerde internationale orde* te versterken en draagvlak voor actie in de internationale veiligheidsarena te creëren?
- Wat kunnen we nog meer doen ter ondersteuning van nationale en internationale pogingen om de *klimaatverandering* af te remmen?
- Hoe kunnen we het *non-proliferatie*regime voor kernwapens en het non-proliferatieverdrag het best ondersteunen?
- Hoe kunnen we de verhouding tussen aanbod van en

vraag naar *energie* op internationaal niveau met succes beheersen gelet op de krapper wordende energiemarkten en de groei van particuliere kernenergie?
- Hoe kunnen we het groeiende gevaar van de *gewelddadige politieke islam* in binnen- en buitenland effectief het hoofd bieden?
- Wat kunnen we nog meer doen om de *mondiale armoede en ongelijkheid* aan te pakken en falende staten en gewelddadige conflicten in de derde wereld te voorkomen?
- Hoe kunnen we ons het best voorbereiden op een eventuele *pandemie* in het VK?
- Hoe kunnen we de *sociaaleconomische kwetsbaarheid* van het VK het best verminderen en zijn kritische nationale infrastructuur versterken?
- Hoe kunnen we beleidsinstrumenten om de oorzaken en gevolgen van *grensoverschrijdende georganiseerde misdaad* aan te pakken het best integreren?
- Wat kunnen we nog meer doen om de veiligheid van kwetsbare voorraden *splijtstoffen* te garanderen?

Dit zijn een aantal urgente kwesties die de *Commission on National Security in the 21st Century* van IPPR zal behandelen en waarvan wij menen dat de regering ze mee moet nemen in haar overwegingen op het gebied van het nationale veiligheidsbeleid.

Ian Kearns en Katie Paintin,
Institute for Public Policy Research (IPPR)

Crises in de 21e eeuw: schreeuwende behoefte aan een nieuwe kosmologie

"Waarom lijkt het altijd alsof we één ramp achterlopen?" [1] Dit is verreweg de belangrijkste vraag achter de rapporten *Failures of Imagination* en *Failures of Initiative*. Het slechte nieuws is dat we crisis na crisis blijven reageren alsof we zodanig geprogrammeerd zijn dat we alleen roepen om meer van hetzelfde: meer standaardantwoorden, meer plannen en meer "command and control". Het goede nieuws is dat er mensen zijn die beginnen in te zien dat de nieuwe kwesties en contexten van de 21e eeuw een grondige omslag vereisen in onze crisiscultuur en -strategie. Net als Magellan in de 16e eeuw [2] hebben we behoefte aan een nieuwe kosmologie. Het is hoog tijd om ons te wagen aan het maken van nieuwe kaarten en nieuwe strategieën, tactieken en onderwijs- en trainingsmodellen uit te broeden [3].

Hier rust de crisisbeheersing

We zijn het er allemaal over eens dat orkaan Katrina een traumatisch fiasco was. Maar we moeten verder kijken dan deze specifieke ramp en er een mondiale boodschap uit distilleren. Ten eerste behoorde Katrina tot de categorie catastrofale gebeurtenissen die steeds gewoner worden: "We moeten rekenen op meer catastrofes van het formaat Katrina, en misschien wel ergere" [4]. Ten tweede worden we in strategisch opzicht overdonderd door dit soort nieuwe ontwikkelingen: "Ons huidige systeem voor binnenlandse veiligheid verschaft niet het nodige kader om de complicaties die catastrofes van de 21e eeuw met zich meebrengen te beheersen" [5]. Ten derde druist het tegen onze cultuur in om de drastische veranderingen >>>

[1] *U.S. House of Representatives, A Failure of Initiative, Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, US Government Printing Office, 15 February 2006 (p. 359).*
[2] *Laurence Bergreen, Over the Edge of the World – Magellan's Terrifying Circumnavigation of the Globe, Harper Perennial, New York, 2004 (pp. 73; 10; 73, 201-202).*
[3] *Patrick Lagadec, 'Over the edge of the world', in: Crisis Response Journal, Volume 3, Issue 4, p. 48-49, September 2007.*
[4] *The White House, The Federal Response to Hurricane Katrina – Lessons Learned, 23 February 2006, p. 65.*
[5] *The White House, idem, p. 52.*

te implementeren die ons in staat stellen de handschoen op te nemen: “Veel ambtenaren weigeren stomweg in te zien dat er fundamentele wijzigingen in de crisisbeheersing nodig zijn” [6].
Op het niveau van tactieken en materieel kan – en moet – er natuurlijk veel gebeuren om onze operationele mogelijkheden te versterken, teksten en plannen te herschrijven, bepaalde gevoelige kwesties als “push”- of “pull”-mechanismen te verduidelijken (we kunnen ons nauwelijks voorstellen welke moeilijkheden de implementatie van een pan-Europees “push”-systeem tot gevolg zou hebben) en om mensen op alle niveaus te trainen. Maar de werkelijke uitdaging zit hem in het feit dat het operationele centrum volledig op de schop moet.

Onze crisiscultuur is verankerd in een achterhaald model. In de twintigste eeuw werd crisis nog omschreven als een acuut probleem dat kon worden opgelost en verholpen door snelle interventie; we moesten gewoon paraat zijn om de nodige middelen in gang te zetten en de normale situatie te herstellen; het probleem was dus specifiek, stond op zichzelf en de context was stabiel. Vandaag de dag kunnen incidenten veel meer ontwrichtend zijn en belangrijker: ze doen zich voor in contexten die fundamenteel instabiel zijn en voortdurend aan verandering onderhevig. Connectiviteit is het *leitmotiv* van onze sterke en zwakke punten en snelheid, onwetendheid, hypercomplexiteit en onvoorstelbaarheid zijn de factoren waar we mee van doen hebben. Elk incident, dus niet alleen rampen van categorie 5, kan onvoorstelbare domino-effecten in gang zetten.

Een heel nieuw spel

Crisisbeheersing gaat inmiddels veel verder dan het reageren op een noodsituatie. En daar moeten we ons aan aanpassen.

Inlichtingen

Ooit hanteerden we een statische aanpak, met vooraf omschreven rampencategorieën, vooraf geplande reacties, vooraf opgezette organisaties en strikte bevelsstructuren. Nu moeten we een nieuw inlichtingenmodel opzetten voor chaotische situaties waarin niets stabiel is en de kleinste wankeling onze denkramen al op hun kop kan zetten en elke actie meerdere reacties oproept.[7] We hadden ooit vaste doctrines waarmee we de juiste implementatie van vaste antwoorden konden garanderen. Nu moeten we

Rapid Reflection Forces [8] in het leven roepen om nieuwe instrumenten voor begrip te ontwikkelen en ons nieuwe wegen te banen door alle terrae incognitae.

Organisatie

Onze plannen waren overzichtelijk georganiseerd volgens het matroesjkamodel, de Russische poppen die elk weer een ander niveau vertegenwoordigden: lokaal, regionaal, nationaal en internationaal. We moeten nu complexere dynamieken creëren en de opeenvolgende logica verlaten: biologie vervangt mechanica.

Leiderschap

We verlieten ons altijd op ambtenaren die op hun beurt weer vertrouwden op een vast corpus aan beste praktijken. Nu moeten we “op alle overheidsniveaus een leiderschapscorps opbouwen (...) dat bestaat uit leiders die innovatie

6 *U.S. House of Representatives, p. xi.*
7 *Mike Granatt’s re-interpretation of Newton’s principle. Personal communication.*
8 *Pierre Béroux, Xavier Guilhou, Patrick Lagadec: ‘Implementing Rapid Reflection Forces’, in: Crisis Response Journal, vol. 3, issue 2, pp. 36-37 & "Rapid Reflection Forces put to the reality test” in Crisis Response Journal, forthcoming, vol 4, issue 2, March 2008.*

niet uit de weg gaan en het initiatief nemen onder extreem zware omstandigheden”[9]

Netwerken

Ooit hadden we behoefte aan duidelijkheid over wie het bevel voerde en wilden we dat uitgebreid in kaart werd gebracht welke stakeholders gecoördineerd moesten worden. Nu moeten we ons instellen op steeds complexere netwerkprocessen en ons realiseren dat voorbereiding, actie en reactie een caleidoscoop aan spelers vereisen. We kunnen niet meer volstaan met “partnerschappen”. Wat we nodig hebben is een “global new deal” waarin de rollen van elke speler fundamenteel gewijzigd zijn en dan vooral de taakverdeling tussen de publieke autoriteiten en de beheerders van vitale netwerken.

Zelfredzaamheid

Onze leiders werden altijd geobsedeerd door het gevaar van paniek onder de bevolking, hoewel de geschiedenis heeft uitgewezen dat burgers zich in tijden van crisis vaak vindingrijk tonen en het hoofd koel houden. Zelfredzaamheid moet dus een vaste factor zijn van alle systemen die we opzetten. Dit betekent dat we niet langer moeten bogen op alleen het principe van *control and command* maar ook moeten leren vertrouwen op de bevolking zelf.

Communicatie

Het hele proces staat of valt met communicatie om mensen met elkaar te verbinden en te kunnen inspelen op zeer snel veranderende situaties. Technische hoogstandjes kunnen niet voorkomen dat ook de elementaire communicatie in gevaar kan komen: “*Interoperabiliteitsproblemen werden ten tijde van Katrina tot op zekere hoogte gemaskeerd door de veel ernstiger problemen van de vernietiging van voorzieningen en stroomuitval.*” [10]. De grootste uitdaging op het gebied van informatie is, wederom, cultureel bepaald. Je kunt weinig uitrichten met satelliettelefoons en Blackberries wanneer de gebruikers verwikkeld zijn in een loopgravenoorlog. Er komt meer bij kijken dan de wijsheid ”*You should not be exchanging business cards when a crisis hits*”: zelfs wanneer de betrokkenen elkaar goed kennen, blijft het de vraag of ze onmiddellijk bereid zijn met bekenden en onbekenden te communiceren wanneer de situatie snel verandert en er geen perfecte informatiestromen of duidelijke bevelsstructuren zijn.

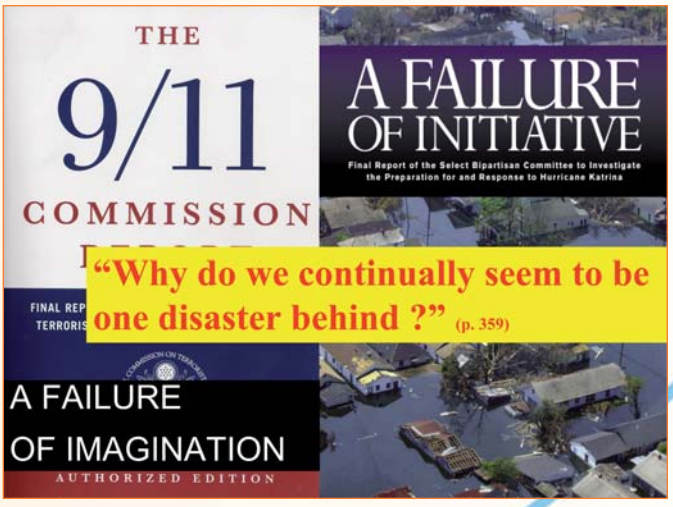
Herstel

In de twintigste eeuw toen de wereld er redelijk stabiel bij lag, draaide alles om het optreden in noodsituaties; terugkeer naar de normale toestand werd geacht min of meer vanzelf te geschieden en was vooral gericht op specifieke schadegevallen. Maar in de onstabiele en complexe wereld van vandaag gaat het niet meer om het “herstel” van muren, bruggen en wegen, zodra de heroïek van reddingsacties weggeëbd is. Het wordt essentieel al jaren van te voren – en dus niet *the day after* – de voorwaarden voor een complexe maatschappelijke textuur te creëren om een nieuwe duurzame dynamiek in een snel veranderende omgeving te bewerkstelligen.

Opleiding en training

We leerden mensen altijd een bekende reeks regels toe te passen. Nu moeten we hen leren om te gaan met het onbekende en creatief te zijn, ook wanneer dat tegenstaat. In het rapport van het Witte Huis staat: “Bij hun opleiding moeten federale ambtenaren er niet voor terugdeinzen te handelen volgens ergst denkbare scenario's die in strijd zijn met ons binnenlandse veiligheidssysteem”[11]. Starheid is fataal in een snel veranderende wereld, waar snelheid en connectiviteit van levensbelang zijn voor veiligheid en betrouwbaarheid. Het is cruciaal anders te gaan denken en handelen. De kwestie van systeemcrises moet hoog op de agenda’s van staatshoofden komen te staan. Laten we daarom niet wachten tot de volgende crisis voordat we strategische initiatieven gaan ontplooien.

Patrick Lagadec,
Directeur Research, Ecole Polytechnique (Paris),
www.patricklagadec.net



[9] *The White House, idem, p. 72.*
[10] *U.S. House of Representatives, idem, p. 165.*
[11] *The White House, idem, p. 73.*

Private ondernemingen worden geconfronteerd met zeer uiteenlopende risico's, die effectief management vergen willen de ondernemingen succesvol kunnen zijn. Bedrijven opereren vaak internationaal in zowel zeer strikt gereguleerde, als in dynamische omgevingen, hebben bij de toelevering te maken met wereldwijde afhankelijkheidsketens en zijn vaak verwikkeld in een hevige concurrentiestrijd. De omvang en complexiteit van de risico's waarmee ondernemingen geconfronteerd worden zijn soms extreem en vormen een enorme uitdaging. Als het bedrijfsleven de risico's niet doorgrondt en er niet adequaat op reageert, kan dat ten koste gaan van de winst en het imago en zelfs tot faillissement leiden.

Risicomanagement in het bedrijfsleven

Ondernemingen kunnen kiezen uit verschillende opties en methoden om hun risico's te beheersen. We zien echter steeds een aantal factoren terugkomen die ondernemingen met een geavanceerd risicobeheersingssysteem kiezen. Ze komen hieronder aan bod.

Geen enkel bedrijf kan onbeperkt in de buidel tasten voor risicomanagement, dus men moet zich concentreren op de waardevolste elementen van de bedrijfsvoering. Het definiëren en meten van waarde is natuurlijk een zeer subjectieve aangelegenheid en zal per onderneming verschillen, maar betreft meestal een aantal tot op zekere hoogte meetbare factoren, zoals winst, imago, merk en groeistrategie. Door de strategische elementen van ondernemingen kwalitatief en kwantitatief te meten komen de activiteiten aan het licht die de meeste waarde opleveren en daarmee kunnen zij prioriteiten vaststellen voor het toespitsen en optimaliseren van het risicobeheer.

Zodra de prioriteiten zijn vastgesteld dient de waardeketen van de activiteit te worden beoordeeld om in kaart te brengen welke afhankelijkheden er zijn wat betreft mensen, technologie, faciliteiten en leveranciers etc. en daarmee de punten en middelen die mogelijk kwetsbaar zijn voor risico's. Wellicht is er al kennis over in huis, maar over het algemeen verdient het aanbeveling de aldus

Risk issue	Risk Avoidance	Risk Mitigation			Crisis Communications	Risk Transfer
Natural Disaster		Business Continuity Management				Property All Risks / Business Interruption
Terrorism		Security Risk Management	Business Continuity Management			Terrorism, Kidnap & Ransom
Fraud and Corruption		Background Screening	Business Intelligence and Investigation			Fidelity Guarantee, Trade Credit
Ethical Risk		Social Accountability	Health and Safety	Environmental		Environmental & Employers' Liability
Infrastructure Risk		IT Security	Business Continuity Management			Business Interruption
Quality and Counterfeiting		Business Intelligence and Investigation	Product Risk / Recall			Legal Expense
Pandemics		Business Continuity Management				(Business Interruption)
Regulatory Risk		Regulatory Research	Business Intelligence and Investigation			Political Risk

Risk management optimisation – Avoidance, mitigation and transfer

Value mapping

verkregen informatie aan te vullen met een gestructureerde risicoanalyse en zo een compleet beeld te krijgen van de gevaren waaraan kritieke middelen blootstaan.

Gefundeerde beslissingen voor het formuleren van een adequate risicomanagementstrategie kunnen worden genomen aan de hand van grondige evaluaties en analyses. Deze moeten worden ondersteund door een inschatting van de risicobereidheid en de tolerantie voor verliezen van de onderneming, zodat objectief wordt vastgesteld welke risiconiveaus aanvaardbaar zijn; de uitkomsten zijn maatgevend voor eventuele latere wijzigingen in processen en investeringen in risicobeheersing, met andere woorden de inzet van middelen wordt geoptimaliseerd. Zo zou vastgesteld kunnen worden dat het incasseringsvermogen of de paraatheid van de onderneming op een bepaald moment buitengewoon hoog is ten opzichte van het tolerantieniveau en voor bepaalde functies verlaagd zou kunnen worden, waardoor kostenbesparingen mogelijk worden. Ook zou besloten kunnen worden het incasseringsvermogen te vergroten door intensiever *business continuity management* (BCM) en een uitgebreidere verzekering, indien het vastgestelde risico onaanvaardbaar wordt geacht.

Deze wijze van risicomanagement kan ook worden toegepast op bedreigingen op individueel niveau, door de kosten-batenanalyse van de voorgestelde methode voor risicomanagement aan te vullen met gegevens over de risicotolerantie van de onderneming. Wanneer we de risico's van natuurrampen als voorbeeld nemen, hebben bedrijven diverse opties om zich hierop voor te bereiden. Zo kunnen ze die vermijden door af te zien van een locatie in een kwetsbaar gebied, gebruik te maken van BCM of het risico af te kopen door middel van een verzekering tegen zaakschade en bedrijfsonderbrekingen. De optimale mix die een onderneming kiest, zal uiteindelijk worden bepaald door factoren als kosten en baten en de gewenste mate van zekerheid. Een verzekering bijvoorbeeld kan de *cashflow* weliswaar op de korte termijn op peil houden, maar geen reputatieschade voorkomen. Het vermijden van risico's zal meer zekerheid bieden, maar dan zal er een financiële veer moeten worden gelaten.

Bedrijven beginnen nu gebruik te maken van technologie om *realtime*-informatie over risico's te verzamelen zodat snel alarm geslagen kan worden bij voor hen relevante bedreigingen die tot waardeverlies kunnen leiden. Dit soort vroegtijdige waarschuwingssystemen kunnen een belangrijke verdedigingslinie vormen om de schadelijke gevolgen van bepaalde risicocategorieën te voorkomen of te beperken.

Matthew Elkington,
vicepresident Marsh Risk Consulting Ltd, London
(matthew.elkington@marsh.com)

Workshop: risicoanalyse

Een van de vier workshops van de conferentie richtte zich op methoden om bedreigingen in te schatten. De twee doelstellingen van deze semi-interactieve workshop waren (1) het presenteren, bespreken, uitwisselen en vergelijken van (innovatieve) methoden, en (2) het initiëren van internationale samenwerking op dit vlak.

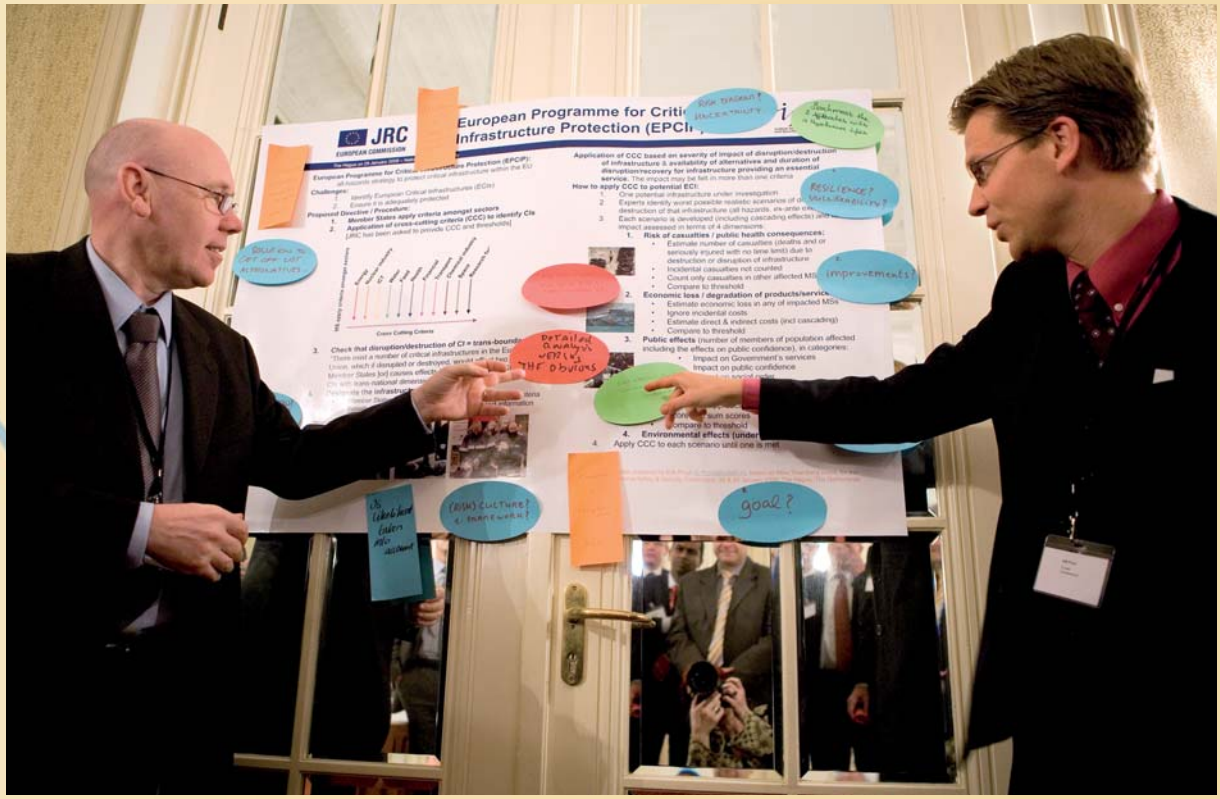
Aan het begin van de workshop werden twee verschillende methoden gepresenteerd: de Nederlandse *Nationale Risico Beoordeling* (NRB) en het *European Programme for Critical Infrastructure Protection* (EPCIP). Beide benaderingen komen hierna separaat aan bod. Deze benaderingen/artikelen worden hier ingeleid middels een bespreking van de redenen om deze presentaties in eenzelfde workshop te houden en een bespreking van interessante overeenkomsten en verschillen. Tenslotte worden enkele workshopdiscussies en -voorstellen kort besproken.

De NRB en EPCIP methoden zijn gepresenteerd omwille van de volgende redenen:

- Deze methoden zijn in het laatste stadium van hun ontwikkeling en zouden nog verbeterd kunnen worden door goede suggesties en kritische opmerkingen.
- Beide methoden zullen binnenkort effectief gebruikt worden. Het EPCIP zal als Europese richtlijn een direct effect hebben op alle EU lidstaten. De Nederlandse NRB zal binnenkort gebruikt worden om het kabinet te informeren over mogelijke risico's en de te verbeteren capaciteiten.
- De ontwikkeling van risicobeoordelingsmethoden vraagt veel tijd en moeite. De gepresenteerde benaderingen zouden bevriende naties en organisaties die (momenteel op het punt zouden staan om dergelijke methoden te ontwikkelen) mogelijkerwijs kunnen inspireren. De ervaring opgedaan in Nederland en het Verenigd Koninkrijk zou andere naties bijvoorbeeld kunnen helpen om zelf op snellere wijze, betere methoden te ontwikkelen en obstakels en valkuilen te vermijden.
- Beide benaderingen bevatten enkele interessante innovatieve aspecten.
- De analyse van overeenkomsten en verschillen tussen benaderingen leidt tevens tot een beter begrip van de benaderingen en van de doelstellingen, omstandigheden en cultuur waaraan ze moeten voldoen.

Een eerste overeenkomst tussen de EPCIP en NRB benaderingen is dat ze 'all hazard' benaderingen zijn, waarin alle bedreigingen beschouwd worden. Een andere overeenkomst is dat ze beide meerdere criteria gebruiken om de impact van incident scenario's op verschillende (kwalitatieve en kwantitatieve) aspecten en dimensies in te schatten. Hoewel Multi-Criteria Analysis (MCA) methoden al meer dan 50 jaar bestaan, is hun toepassing op de (Nationale) Veiligheid relatief nieuw. Beide benaderingen stellen hoge – maar licht verschillende – eisen aan de vele scenario's die ontwikkeld moeten worden. Het scenario-ontwikkelingsproces is daarom van cruciaal belang.
De EPCIP en NRB benaderingen verschillen aan de andere kant ook aanzienlijk van elkaar. De verschillen in niveau (het EU niveau versus het nationale niveau) en de reikwijdte (altijd grensoverschrijdend versus vooral nationaal) spreken voor zich. De verschillen in motief en focus van de analyse zijn waarschijnlijk minder duidelijk. Het motief voor de EPCIP is de bescherming van Europese vitale infrastructuren, en de focus van de analyse is de identificatie van deze Europese Vitale Infrastructuren. Motieven voor de NRB zijn enerzijds de verbetering van de capaciteiten om voorbereid te zijn op en om te gaan met potentieel grote risico's/rampen, en anderzijds de verbetering van de samenwerking tussen ministeries. De focus van de analyse is daarom de gemeenschappelijke identificatie en de robuuste classificatie van de breedst mogelijke verzameling van potentieel catastrofale risico-scenario's en de identificatie van de benodigde capaciteiten die verbeterd zouden moeten worden om ermee om te gaan.

De gebruikte MCA methoden en technieken verschillen dientengevolge ook aanzienlijk. Het EPCIP is een minimumdrempel benadering waarbij multidimensionale effecten niet geaggregeerd worden. Dit betekent dat de ordegrootte van de impact – buiten de afweging of ze de drempelwaarde overstijgen of niet – niet van belang zijn, en dat er geen compensatie optreedt tussen effecten op verschillende criteria. Een infrastructuur zal bijvoorbeeld niet als *Europees vitaal* geklasseerd worden als alle impacten nipt onder de drempelwaarden vallen. In de Nederlandse benadering wordt de ordegrootte van de impact op de verschillende criteria wel beoordeeld en worden de multi-dimensionale effecten deels geaggregeerd, hetgeen inhoudt dat er compensatorische effecten optreden tussen criteria, die nauwgezet geanalyseerd worden.
De impactcriteria verschillen ook: de EPCIP criteria zijn



speciaal gedefinieerd om grensoverschrijdende effecten in te schatten, terwijl de Nederlandse criteria speciaal gedefinieerd zijn om – voor Nederland belangrijke – *nationale* effecten in te schatten.
De EPCIP scenario's moeten specifiek zijn en omvatten directe en indirecte effecten (*cascading effects*), terwijl de Nederlandse scenario's zo generiek mogelijk en tegelijkertijd specifiek genoeg moeten zijn om enkel de directe effecten te scoren.
Uitgebreide gevoeligheidsanalyses (onzekere scores en gewichten) en robuustheidsanalyses (verschillende methoden) zijn – gegeven het generieke karakter van de scenario's en de gebruikte MCA methoden – van groot belang in de Nederlandse methode.
Beide benaderingen weerspiegelen in feite de cultuur en het proces waaruit ze ontstaan zijn. De EPCIP benadering kan beschouwd worden als een compromisbenadering, terwijl de NRB een typisch Nederlandse, op consensus gerichte benadering is. De Nederlandse methode is ontwikkeld door een team van vertegenwoordigers van verschillende departementen, kennisinstituten (planbureaus, universiteiten, think-tanks) en het bedrijfsleven.

Na de presentatie van deze twee benaderingen, volgde een interactieve post-it activiteit en een discussie van de opmerkingen. De discussie was vooral gecentreerd rond vragen als:

- Dient men deze benaderingen te richten op *veiligheid* en/of *beveiliging*?
- Zijn deze benaderingen fundamenteel gevolg- en/of *dreigingsgeoriënteerd*? Wat zou van complementaire benaderingen geleerd kunnen worden?
- Voegt de gedetailleerde analyse waarde toe?
- Hoe kunnen fundamenteel verrassende risico's ook beschouwd worden?
- Zou – en hoe zou – een vruchtbare samenwerking tussen en binnen regionale, nationale, en lokale niveaus tot stand gebracht kunnen worden?
- Zou informatie betreffende methoden gedeeld kunnen worden?
- Zou informatie betreffende scenario's gedeeld kunnen worden?
- Zouden de benaderingen ontwikkeld in een bepaalde context, rechtstreeks in een andere context toegepast kunnen worden?

Tenslotte werd een aantal ideeën besproken om de internationale samenwerking op het vlak van de risicobeoordeling te verbeteren. Er werd onder meer voorgesteld om netwerken (*networks of excellence*) op te zetten, om follow-up conferenties en workshops betreffende risicobeoordelingsmethoden te organiseren, om de samenwerking naar andere organisaties en niveaus uit te breiden, en ten slotte om de huidige stimulansen voor internationale samenwerking te verbeteren.
Deze conferentie (en workshop) zouden vanuit dat opzicht het begin kunnen zijn van een vruchtbare samenwerking op het vlak van de risicobeoordeling.

dr. Erik Pruyt,
Technische Universiteit Delft

Nationale Risicobeoordeling: de Nederlandse aanpak

Dit artikel beschrijft de methodiek voor de Nationale Risicobeoordeling (NRB) in Nederland zoals deze door een expertgroep in 2007 is ontwikkeld. De NRB methodiek verschaft de Nederlandse regering een omvattende en gekwalificeerde ondersteuning bij het prioriteren van risico's op nationale schaal met het doel om op consistente en reproduceerbare wijze het planningsproces vorm te geven voor de vereiste taken en capaciteiten ingeval de geïdentificeerde risico's daadwerkelijk optreden. De methodiek is met succes toegepast voor een geselecteerd aantal incidentscenario's. De methodiek wordt in 2008 verder aangescherpt.

Inleiding

De Nederlandse regering heeft het besluit genomen een Strategie Nationale Veiligheid te ontwikkelen met het doel de onderstaande vijf geselecteerde nationale belangen optimaal te beschermen tegen potentiële grootschalige risico's (incidentscenario's):

- territoriale veiligheid;
- fysieke veiligheid;
- economische veiligheid;
- ecologische veiligheid;
- sociale en politieke stabiliteit.

Het belangrijkste doel van de Nationale Risico Beoordeling, welke deel uitmaakt van het proces om een Strategie Nationale Veiligheid te ontwikkelen, is de Nederlandse regering inzicht te verschaffen in de onderlinge rangschikking van de geïdentificeerde incidentscenario's wat betreft het afbreukrisico – in termen van waarschijnlijkheid en omvang – voor de nationale belangen.
De volgende randvoorwaarden voor de ontwikkeling van de NRB methodiek zijn gesteld:

- de methodiek is geschikt voor alle soorten risico's, zowel gevaren als (terroristische) dreigingen;
- het rangschikken van de geselecteerde risico's (incidentscenario's) moet gebaseerd worden op de integrale weging van de aantasting van zeer ongelijksoortige belangen.

Risicoanalyse is het proces dat resulteert in de rangschikking van ongewenste gebeurtenissen (incidentscenario's) op basis van hun waarschijnlijkheid en potentiële schadeomvang.
Risicoanalysemethoden zijn voor onderscheiden toepassingsgebieden ontwikkeld, bijvoorbeeld industriële veiligheid, risico management, treasury, besliskunde, en staan uitvoerig beschreven in de literatuur.

Niettemin vormt de ontwikkeling van de NRB methodiek een grote uitdaging vanwege:

- de integratie van zeer verschillende schadegevolgen (bijvoorbeeld verlies van territorium tegenover aantal doden);
- het bepalen van de waarschijnlijkheid voor onbekende risico's (bijvoorbeeld nieuwe terroristische dreigingen), extreme catastrofes (geen statistische gegevens), of gebeurtenissen die zich ontwikkelen (bijvoorbeeld klimaatverandering);
- de complexiteit van het rangschikken van incidentscenario's op basis van de uitkomsten voor waarschijnlijkheid en schadeomvang.

Op basis van de poster zullen in de volgende paragrafen de belangrijkste stappen van de NRB methodiek worden toegelicht.

Bepaling schadeomvang (impact)

De eerste stap in het proces van Nationale Risico Beoordeling betreft de identificatie, selectie en beschrijving van de incidentscenario's. Daarbij kan bijvoorbeeld gedacht worden aan overstroming, pandemie, terroristische aanslag of grootschalige energie uitval. Voor 2007 zijn door expertgroepen 13 scenario's uitgewerkt. Ieder scenario wordt uitgebreid gedefinieerd, waarbij het risico is vertaald in termen van zeer ernstig of maximaal geloofwaardig. Alle scenario's zijn zodanig ernstig dat een of meer van de vitale belangen geschaad wordt en daarmee de nationale veiligheid in het geding is. De scenario's moeten zodanig informatief zijn dat het mogelijk is waarschijnlijkheid en schadeomvang te bepalen.
De analyse van de schadeomvang omvat de vijf gedefinieerde nationale belangen. Ieder belang is vertaald in één of meer schadecriteria, die gezamenlijk representatief worden geacht voor de schade. In totaal zijn 10 schade-

criteria gedefinieerd. *Fysieke veiligheid* wordt bijvoorbeeld gerepresenteerd door de schadecriteria doden (1), gewonden (2) en fysiek lijden (3). Elk schadecriterium is op zodanige wijze beschreven dat de omvang eenvoudig gescoord kan worden. Doden is bijvoorbeeld gedefinieerd als het aantal mensen dat onmiddellijk of binnen een jaar sterft als direct gevolg van het beschreven incidentscenario. Voor alle schadecriteria zijn 5 klassen gedefinieerd, uiteenlopend van A (minimum schade) tot E (maximum schade). Bijvoorbeeld het schadecriterium doden: klasse A representeert 0-10 doden, en klasse E representeert 10.000 doden of meer. Ingeval een individueel schadescenario in het geheel geen afbreuk doet aan een vitaal belang respectievelijk schadecriterium dan wordt de score 0 toegekend (niet van toepassing). Een pandemie heeft bijvoorbeeld geen enkele invloed op het vitaal belang Ecologische Veiligheid, met als gevolg dat het schadecriterium langdurige ecologische verstoring van flora en fauna de score 0 krijgt.

Multi Criteria Analyse

Om de scores voor de 10 schadecriteria 'op te tellen' tot één score voor de schadeomvang wordt gebruik gemaakt van Multi Criteria Analyse (MCA).
Om te voorkomen dat op voorhand methodologische keuzes gemaakt worden die invloed kunnen hebben op het eindresultaat – de rangschikking van de incidentscenario's naar schadeomvang – is besloten om:

- drie verschillende MCA methodes toe te passen:
  - gewogen som methode – een puur kwantitatieve utiliteitsfunctie benadering;
  - medaille methode – een puur kwalitatieve benadering;
  - Evamix methode – een gecombineerde kwalitatieve/kwantitatieve benadering;
- vijf verschillende preferentieprofielen te definiëren. Als uitgangspunt wordt het profiel gehanteerd dat hetzelfde gewicht toekent aan alle vijf vitale belangen. Daarnaast zijn 4 karakteristieke sociaal/culturele preferentieprofielen gedefinieerd die ieder verschillende gewichten toekent aan de vitale belangen respectievelijk schadecriteria;
- verschillende weging toe te passen om A, B, C, D, E scores te herberekenen, variërend van lineair tot exponentieel.

Om een beter begrip te krijgen over de onzekerheid en robuustheid van het resultaat zijn de berekeningen uitgevoerd voor alle denkbare combinaties van MCA methoden, preferentieprofielen, gewichten, onzekerheidsintervallen voor individuele schadecriteria, enzovoorts. Uit de berekeningen blijkt dat het resultaat voor de 2007 scenario's als robuust kan worden beschreven. De rangschikking varieert slechts in beperkte mate afhankelijk van de gekozen combinatie.

Bepaling waarschijnlijkheid

Alle gedefinieerde incidentscenario's kunnen gekarakteriseerd worden als onzeker voorval, en het risico kan dus – naast schadeomvang – ook gekarakteriseerd worden door de waarschijnlijkheid. Om in staat te zijn de >>>

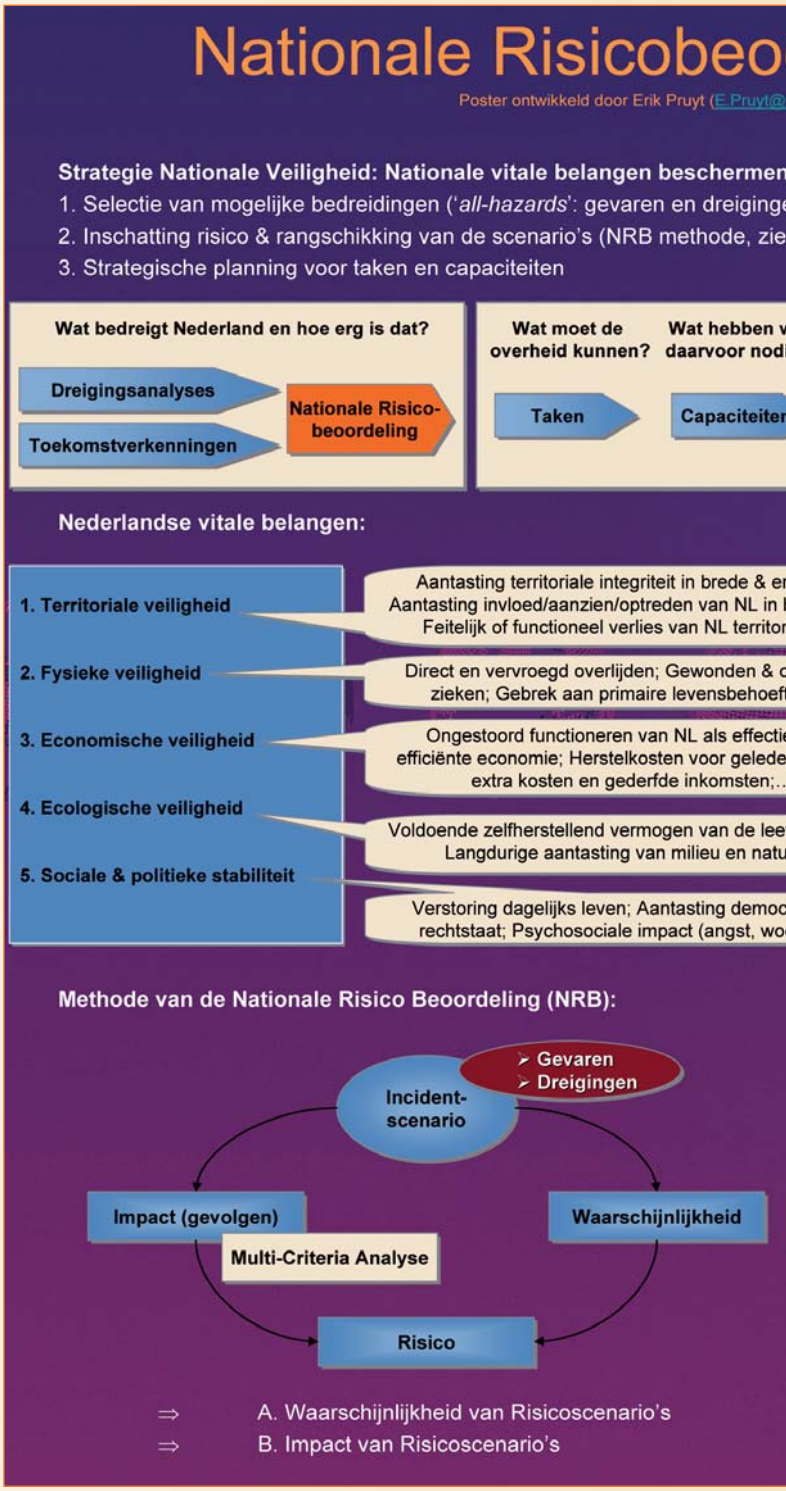
incidentscenario's te prioriteren naar risico moet de waarschijnlijkheid afgezet worden tegen de schadeomvang. De waarschijnlijkheid wordt bepaald voor een periode van vijf jaar, en wordt – evenals de schadeomvang – gepresenteerd op een 5-puntsschaal: klasse A-B-C-D-E. Klasse A representeert 'minst waarschijnlijke gebeurtenis' , klasse E representeert 'meest waarschijnlijke gebeurtenis'. Vanwege het feit dat de meeste incidentscenario's een lage kans van optreden hebben, is ervoor gekozen dat de onderlinge weging van de schalen een exponentieel karakter dragen. Voor de kwantitatieve schaal wordt een factor 10 gehanteerd. Een bijkomend gevolg is dat de schaalverdeling vrij robuust is, en compenseert voor het belangrijkste probleem bij het bepalen van de waarschijnlijkheid, namelijk het gebrek aan kennis en statistische gegevens. Het bepalen van de waarschijnlijkheid voor de incidentscenario's zal sterk afhankelijk zijn van de mening van experts, het proces om kennis aan de experts te onttrekken zal zorgvuldig dienen te gebeuren.

Belangrijkste vraag is: welke incidentscenario's vragen prioriteit?

Voor dreigingen ('malicious events') en gevaren ('non-malicious events') zijn verschillende schalen gehanteerd. De waarschijnlijkheid voor gevaren wordt direct gescoord op basis van de gedefinieerde kwantitatieve en kwalitatieve schaal; hierbij wordt gebruik gemaakt van historische gegevens, modelberekeningen, experts enzovoorts. Statistiek en historische gegevens zijn van weinig betekenis voor het bepalen van de waarschijnlijkheid voor dreigingen. De beschreven dreigingen hebben (nog) niet plaatsgevonden. De waarschijnlijkheid wordt gebaseerd op beschikbare kennis en onderzoek bij AIVD, KLPD e.a. Het resultaat van deze dreigingsanalyses resulteert in een waarschijnlijkheidsscore aan de hand van een kwalitatieve klasse aanduiding. De score kan nog bijgesteld worden op basis van een analyse van de kwetsbaarheid voor het dreigingscenario. De kwetsbaarheid is een maat voor het verwachte succes met betrekking tot het uitvoeren van de dreiging, en is direct gekoppeld aan de reeds getroffen beveiligingsmaatregelen. Indien de kwetsbaarheid laag wordt ingeschat, wordt de waarschijnlijkheid een klasse verlaagd (C wordt B); in geval de kwetsbaarheid hoog scoort, wordt de waarschijnlijkheid een klasse verhoogd (C wordt D).

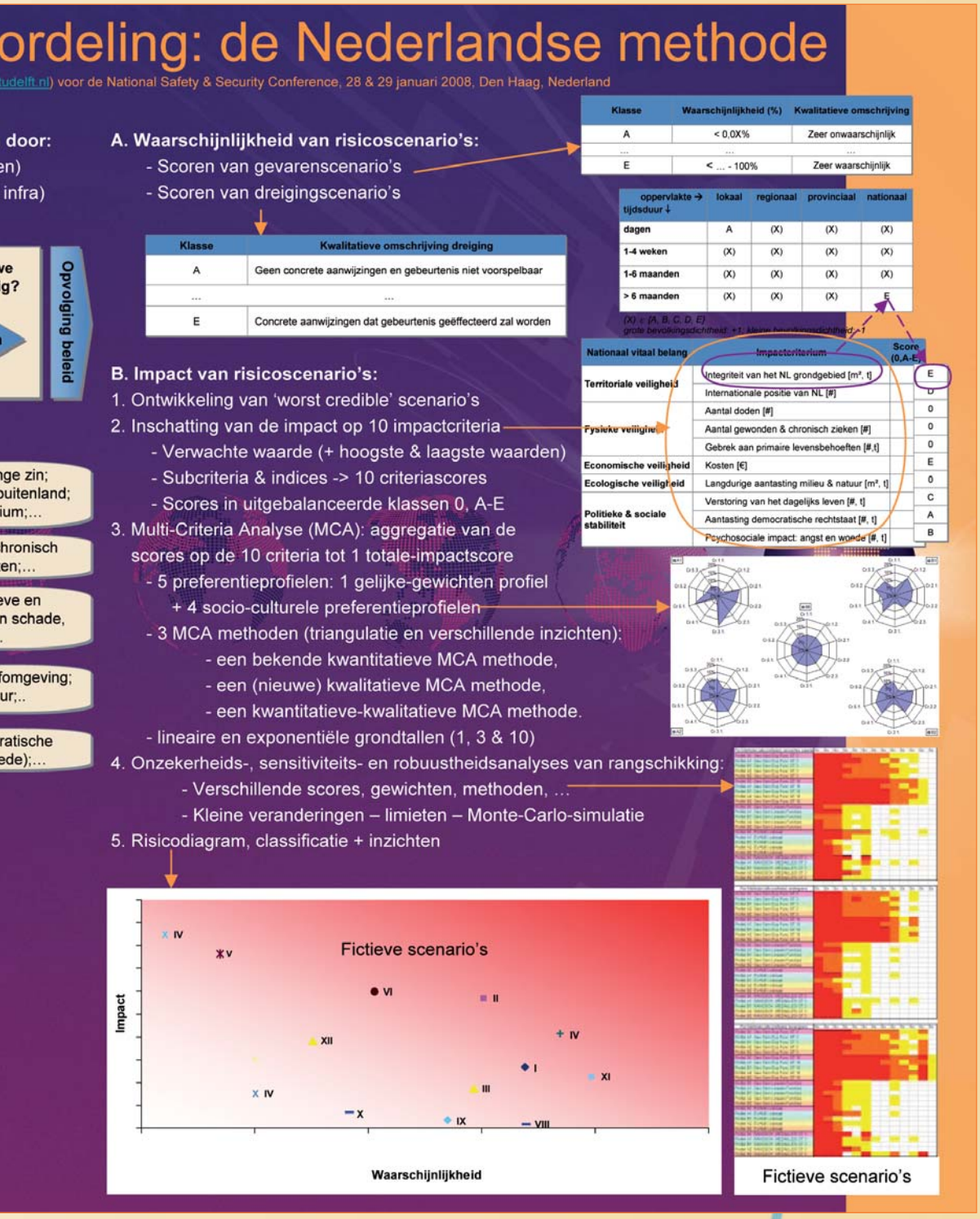
Risicodiagram

Met het doel de totale risicoscore voor een incidentscenario zichtbaar te maken worden de scores voor schadeomvang en waarschijnlijkheid geplot in een zogeheten risicodiagram.



De interpretatie van het volledige risicodiagram is niet eenvoudig. Belangrijkste vraag is: welke incidentscenario's vragen prioriteit? Daarbij dient rekening gehouden te worden met een aantal formele regels:

- Risico is een functie van waarschijnlijkheid en schadeomvang; in de meest eenvoudige vorm risico = waarschijnlijkheid x schadeomvang;
- Extreme scores voor de schadeomvang mogen niet genegeerd worden, ongeacht de score voor waarschijnlijkheid;
- Optimaliseren van de nutsfunctie, dit is het



maximaliseren van de risicoreductie die gerealiseerd wordt door de inzet van de capaciteiten.

Daarnaast spelen ook subjectieve overwegingen een rol bij de interpretatie van het risicodiagram:

- Het uitspreken van preferenties voor specifieke nationale belangen en schadecriteria;
- Prioriteit geven aan waarneembare maatschappelijke trends;
- Beperkingen opgelegd door budgetruimte en tijdplanning, enzovoorts.

Het gevolg is dat het groeperen en rangschikken van de incidentscenario's met het doel het planningsproces voor taken en capaciteiten te ondersteunen geen eenvoudige taak is; belangrijk is de toetsingsregels duidelijk te identificeren en vast te leggen.

Jasper van der Horst,
Aon Global Risk Consultants
Erik Pruyt,
Technische Universiteit Delft

Bescherming van de vitale infrastructuur: de Europese aanpak

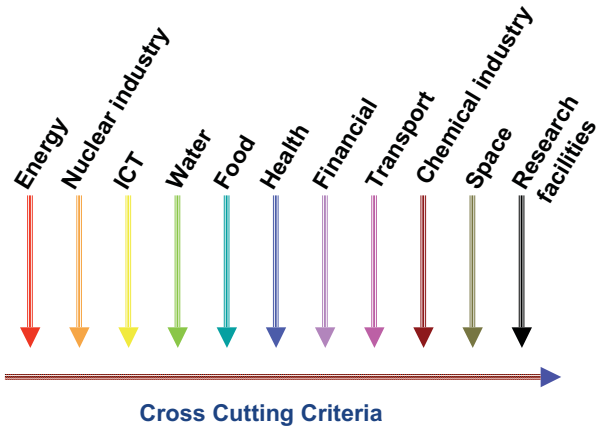
Uit de gruweldaden van 11 september 2001 in New York en de bomaanslagen op de treinen in Madrid in 2004 blijkt dat terroristen zowel mensen als infrastructuur tot doelwit kiezen. Na deze gebeurtenissen heeft de Europese Raad de Europese Commissie verzocht een allesomvattende strategie ter bescherming van vitale (ook wel "kritieke") infrastructuur[1] binnen de Europese Unie te formuleren.

In het kader van deze strategie heeft de Europese Commissie een richtlijn voor het inventariseren en aanwijzen van Europese vitale infrastructuur voorgesteld alsmede voor het beoordelen van de noodzaak de bescherming ervan te verbeteren[2]. Hoewel we terroristische dreigingen als een prioriteit aanmerken, moeten we onderkennen dat ook natuurrampen of ongevallen vergelijkbare gevolgen kunnen hebben, namelijk ontwrichting of vernietiging van de infrastructuur. De bescherming van de vitale infrastructuur wordt daarom gekenmerkt door een integrale benadering die op alle vormen van gevaar gericht is.

Europees programma bescherming vitale infrastructuur

Binnen de Europese Unie is er mogelijk infrastructuur waarvan ontwrichting of vernietiging twee of meer lidstaten zou kunnen treffen. Ook uitval van de infrastructuur in de ene lidstaat zou gevolgen kunnen hebben in de andere. Dergelijke infrastructuur met grensoverschrijdende dimensies waarvan uitval ingrijpende gevolgen zou kunnen hebben moet worden aangeduid en aangewezen als Europese vitale infrastructuur (ECI, European Critical Infrastructures). Juist vanwege die transnationale dimensie zou een integrale pan-Europese benadering bij het onderzoeken en inventariseren van de zwakke en kwetsbare plekken en lacunes in de bescherming een zinvolle aanvulling zijn op en toegevoegde waarde verlenen aan de nationale programma's die de lidstaten reeds hanteren ter bescherming van hun vitale infrastructuur.

In de voorgestelde richtlijn wordt elke lidstaat verplicht sectoren te onderwerpen aan bepaalde criteria en daar vervolgens sectoroverschrijdende (ook wel "cross-cutting") criteria op toe te passen om zo de infrastructuur te identificeren die als ECI kan worden aangewezen. Aangezien deze inventarisatie door de lidstaten zelf geschiedt aan de hand van sectorale criteria, kan noch binnen sectoren noch binnen lidstaten een coherente en uniforme identificatie van ECI worden gewaarborgd. Om inconsistentie bij de identificatie te voorkomen moeten de lidstaten vervolgens een reeks sectoroverschrijdende criteria toepassen op de eerder geïdentificeerde infrastructuur. Met behulp van de sectoroverschrijdende criteria dienen de uitkomsten te worden geharmoniseerd.



De 11 sectoren van de Europese infrastructuur en de horizontale of sectoroverschrijdende criteria.

[1] *Vitale infrastructuur kan in zijn algemeenheid worden omschreven als het geheel van fysieke faciliteiten en faciliteiten op het gebied van informatietechnologie, alsmede diensten en andere voorzieningen waarvan de onderbreking of vernietiging ernstige gevolgen zal hebben voor de gezondheid, veiligheid en/of het economisch welzijn van burgers.*

[2] *Een Richtlijn inzake de inventarisatie van de Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren, COM(2006) 787 definitief, 12 december 2006.*

Mislukte aanslag op de luchthaven van Glasgow (© Reuters 30 juni 2007)

Sectoroverschrijdende criteria

In de richtlijn worden vier categorieën van mogelijke schadelijke gevolgen voor de maatschappij omschreven. Hiermee kan worden bepaald welke maatschappelijke gevolgen het uitvallen van infrastructuur minimaal moet hebben om als ECI te worden geclassificeerd.
De vier categorieën die in de richtlijn worden genoemd zijn:

- de kans slachtoffers te veroorzaken en de mogelijke gevolgen voor de volksgezondheid (raming van het aantal doden of zwaargewonden), door vernietiging of uitval van infrastructuur;
- economische gevolgen (omvang van de economische schade en/of aantasting van producten en/of diensten). Raming van de economische schade ten gevolge van de vernietiging of uitval van infrastructuur in de (overige) getroffen lidstaten;
- gevolgen voor de bevolking (aantal burgers die getroffen worden, met inbegrip van de gevolgen voor het vertrouwen van de bevolking);
- gevolgen voor het milieu.

In de richtlijn staat ook expliciet dat bij het toepassen van de sectoroverschrijdende criteria ook de beschikbaarheid van alternatieven en de duur van de uitval of hersteltijd van een dienst in aanmerking moeten worden genomen. Het aantal slachtoffers en de mogelijke economische schade kunnen worden geschat, maar er is geen methode bekend voor het kwantificeren van gevolgen voor het publiek. Daarom is gekozen voor een kwalificerende aanpak, waarbij vijf verschillende categorieën van gevolgen aan de orde komen:

- gevolgen voor de diensten van de overheid;
- invloed op het vertrouwen van de bevolking;
- gevolgen voor de openbare orde;
- getroffen bevolkingsgroep;
- geopolitieke gevolgen.

Deze worden geïnventariseerd, van een score voorzien en afgezet tegen een vooraf vastgestelde drempelwaarde.

Voor de infrastructuur die zij willen gaan onderzoeken schetsen de lidstaten eerst de ergst denkbare, realistische scenario's die zich bij uitval of vernietiging kunnen voordoen . Elk scenario wordt uitgewerkt (waar mogelijk met secundaire gevolgen) met zijn gevolgen in vier dimensies (kans op slachtoffers, economische en milieuschade en gevolgen voor de bevolking). Deze sectoroverschrijdende criteria worden toegepast op elk scenario totdat er aan een wordt voldaan. Deze drempelwaarden worden zodanig vastgesteld dat alleen die onderdelen van de infrastructuur die bij uitval grote gevolgen zouden hebben als vitaal of kritiek worden aangemerkt. Een onderdeel van de infrastructuur dat zowel de sectorale als sectoroverschrijdende criteria overschrijdt en bij uitval of vernietiging grensoverschrijdende gevolgen zou hebben wordt als ECI oftewel als Europese vitale infrastructuur aangemerkt.

Michael Thornton,
Researcher, Joint Research Centre of the European Commission (Ispra, Italy)

Workshop: Hoe kunnen we bedreigingen het hoofd bieden?

Facilitator: Neil Ellis, Consultant, PA Consulting Group

Sprekers:
- **Bengt Sundelius, Chief Scientist, Swedish Emergency Management Agency (SEMA)**
- **Garry Hindle, Head of Security and Counter-terrorism, Royal United Services Institute (RUSI)**

De centrale vraag – Hoe kunnen wij bedreigingen het hoofd bieden? – werd in deze workshop vanuit verschillende invalshoeken benaderd: enerzijds het voorbereiden van een effectieve reactie op bepaalde situaties en anderzijds het nemen van maatregelen om die bedreigingen te verminderen. Beide sprekers brachten verschillende technieken voor het voetlicht en kwamen met voorbeelden van mogelijke strategieën om effectiever op bedreigingen te kunnen inspelen.

Aspecten van leiderschap

Sundelius plaatste vraagtekens bij het relatieve belang van preventie en voorbereiding. Hoewel preventie zeker zinvol is, kun je lang niet alles voorkomen. Daarom is het essentieel goed voorbereid te zijn. Er bestaat duidelijk een subtiel evenwicht tussen investeren in preventie en investeren in voorbereiding.
Gezien de nadruk op voorbereiding onderstreepte de spreker het cruciale belang van goed leiderschap in crisis-situaties. Als er veel op het spel staat, verwacht het publiek daadkracht van een leider – ongeacht diens functioneren in zijn dagelijks werk. Hij wees er ook op dat crises niet alleen als risico's of bedreigingen moeten worden gezien, maar ook kansen bieden. Slimme leiders treden effectief op in specifieke situaties om zo hun rol te legitimeren.
Sundelius gaf vervolgens een overzicht van wat hij de zes aspecten van leiderschap noemde:
- doorgronden – diagnose stellen van de situatie;
- besluiten nemen – strategische keuzes maken;
- opinie vormen – kaders bieden voor breed gedeelde opvattingen;
- verantwoording afleggen – aanvaarden van eigen verantwoordelijkheid;
- beëindigen – de kwestie afronden;
- leren – kritische reflectie op en aanpassing van eigen optreden.

Samenvattend stelde hij dat het voor een effectieve aanpak van risico's noodzakelijk is de verantwoordelijken te ondersteunen en hen te stimuleren te investeren in voorbereiding. Er is behoefte aan een Europa-breed stelsel van crisisbeheersingssystemen die elkaar niet blokkeren, maar versterken. Dit is van essentieel belang, zeker gezien het verwachte overschot aan kwetsbaarheid en het tekort aan capaciteit in de komende tien jaar.

Lokaal en mondiaal meer samenwerken

Hindle gaf een voorbeeld van een lopend initiatief dat erop is gericht bedreigingen te verminderen via de burgers zelf. Hij gaf aan dat het, in algemene zin, steeds belangrijker wordt de burger op lokaal niveau te benaderen en tegelijkertijd intensiever samen te werken op mondiaal niveau. In een wereld vol bedreigingen kunnen de burgers een hoofdrol vervullen als we juist op lokaal niveau meer bevoegdheden toekennen.
Voorts wees hij erop dat de communicatie tussen de politie en moskeeën in het Verenigd Koninkrijk is verbeterd sinds de bomaanslagen van 7 juli 2005. Er zijn ook meer informanten geworven en de noodzaak van verdere ontwikkeling en uitbreiding van dergelijke relaties is inmiddels evident. Hij noemde ook het Pathfinder-initiatief dat de Britse regering begin 2007 lanceerde om moslims in staat te stellen zelf op te treden tegen extremisme, om een formeel kader te bieden voor de betrekkingen na 7 juli 2005 en om vernieuwende ideeën vanuit de gemeenschap te stimuleren. In 2007/2008 werd vijf miljoen pond geïnvesteerd in het opbouwen van relaties met islamitische jongeren – de groep die het grootste risico loopt te radicaliseren – en islamitische vrouwen, die een cruciale en invloedrijke rol spelen binnen hun gemeenschap.

De discussie spitste zich aanvankelijk toe op het inkaderen van de publieke opinie en hoe je dit in de praktijk aanpakt door je bewust te zijn van de gevolgen van handelen of niet handelen. Bij crisisbeheersing is het van belang de aandacht niet uitsluitend te vestigen op de actuele situatie, maar ook oog te hebben voor de betekenis daarvan voor de gemeenschap.

De discussie richtte zich vervolgens op het gesignaleerde overschot aan kwetsbaarheid en tekort aan capaciteit en

v.l.n.r.: Sundelius, Ellis en Hindle

het effectieve beheer daarvan. Volgens de deelnemers kun je wel kwesties aan de orde stellen, maar wordt je dat door politici niet in dank afgenomen als je niet ook de oplossing biedt. Het gevaar bestaat echter dat men wordt overstelpt door de vele potentiële risico's. Er moeten hulpmiddelen voor crisisbeheersing voorhanden zijn en de risico's moeten integraal worden benaderd om de gevolgen in goede banen te kunnen leiden. Een belangrijk punt was dat het volgens de deelnemers zaak is goed te weten hoe je hulp van andere landen kunt krijgen. Aan welke specialistische kennis bestaat behoefte en waar kan die kennis worden verworven? De nationale risicobeoordelingen moeten aan overheden worden voorgelegd, zodat die zorgvuldig kunnen afwegen waar de prioriteiten moeten komen te liggen.

In het verlengde hiervan werd het idee van de "sluipende crisis" aangedragen. Klimaatverandering is hier volgens de deelnemers een goed voorbeeld van; het is immers moeilijk geld vrij te maken voor de voorbereiding op iets wat nog niet heeft plaatsgevonden. Als het gaat om bedreigingen als terrorisme zijn veel landen geneigd zich uitsluitend te richten op nationale veiligheidsplannen, maar de voorbereiding op bijvoorbeeld klimaatverandering vereist een internationaal mechanisme. Bij het aantrekken van investeringen is het van cruciaal belang niet alleen de bedreiging zelf, maar ook de gevolgen van die bedreiging voor het voetlicht te brengen.

Ten slotte was men van mening dat er behoefte is aan een discussie omtrent het gebruik van terminologie. Sinds "veiligheid" is veranderd in "crisisbeheersing" wordt de discussie alleen nog achter gesloten deuren gevoerd. Misschien zou er onderscheid gemaakt moeten worden tussen nationale veiligheid en maatschappelijke veiligheid.

Workshop: Met welke bedreigingen moeten we rekening houden? *(foresight)*

Facilitator: Stephan de Spiegeleire, Director Defence Transformation, The Hague Centre for Strategic Studies

Sprekers

- **Peter Schwartz, Founder and chair Global Risk Network**
- **Michael Oborne, Director, Advisory Unit on Multidisciplinary Issues, OESO**

Peter Schwartz: de kunst van het vooruitzien – strategisch denken en toekomstscenario's

Het inspelen op bedreigingen is voor veel organisaties een hele uitdaging. Wat bedreigingen volgens sommigen echter vooral gevaarlijk maakt is niet zozeer het onvermogen ze te zien, maar ze te onderkennen. Het onderkennen van een bedreiging betekent immers ook dat we actie moeten ondernemen. De machthebbers gaan vaak gebukt onder een gebrek aan verbeeldingskracht en aan kritische reflectie over hun eigen denkpatronen. Een extern perspectief is dan ook essentieel om dit te doorbreken.

Het opstellen van scenario's is iets anders dan het voorspellen van de toekomst. Scenario's maken ons alert op trends die zich voordoen. Het voordeel van scenario-planning is dan ook niet gelegen in toekomstvoorspellingen, maar in het stimuleren van maatregelen. Scenario's >>>

bieden daarnaast een richting aan strategische gesprekken, op basis waarvan we de verschillende onderdelen van beveiligingsorganisaties op één lijn kunnen brengen.

Er werden verschillende nieuwe bedreigingen en veranderende trends gepresenteerd en besproken, waaronder de fragmentatie van de politieke centra, de impact van na-ijleffecten, de gevolgen van een kenniseconomie, de privatisering van het buitenlands beleid, vorderingen in de biologie en zorgen omtrent de toegang tot water.

v.l.n.r.: De Spiegeleire, Schwartz en Oborne

Michael Oborne

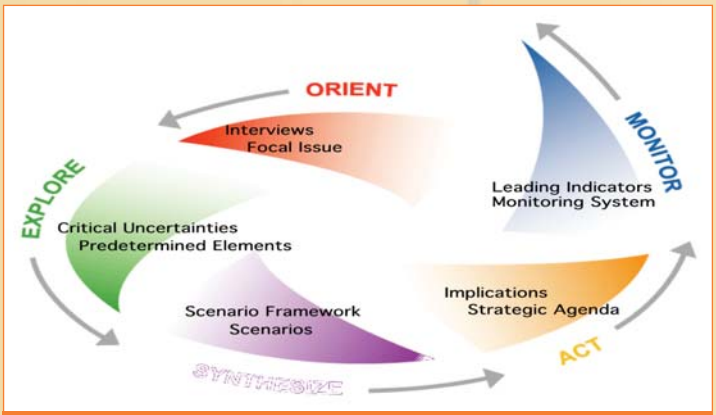
Het belangrijkste probleem waar zij die vooruitzien mee kampen, zo werd gesteld, is niet zozeer de boodschap maar eerder de bewustwording van het publiek. Er werden toekomstbeelden geschetst en besproken in vier categorieën: Merlijn, Cassandra, Dr Strangelove en de Hofnar.
Er werd een aantal beleidsproblemen voor de middellange termijn besproken, ten aanzien van onder meer de risico's van de financiële markten, de vervuiling van de zee en de gevolgen daarvan voor de visstand, migratie (zowel immigratie als emigratie), wijzigingen in waarden als identiteit en sociale cohesie en onduidelijkheid over de situatie in India en China zodra hun economieën tot volle wasdom zijn gekomen.

Discussie

In de discussie kwamen de volgende punten naar voren:

a De planning van voorspelbare trends is al grotendeels rond. Er moeten nu belangrijke beslissingen worden genomen over investeringen omtrent de minder voorspelbare vraagstukken.

b Er is overtuigingskracht nodig om mensen aan te zetten tot het nemen van beslissingen en dat kost tijd. Het verdient de voorkeur geen dingen voor te schrijven, maar mensen de middelen in handen te geven waarmee ze de indicatoren zelf kunnen vaststellen.



The scenario thinking process

c Voor het opstellen van een lijst van trends moet een systematische aanpak worden gevolgd, met inbegrip van literatuurstudie, interviews en een 'netwerk van opvallende mensen' waar signalen van de frontlinie van veranderingen kunnen worden opgevangen. De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) gaat uit van een dialoog met 117 instellingen op basis waarvan een uitvoerige lijst van onderwerpen wordt samengesteld. De OESO maakt gebruik van een wereldwijd forum van wetenschappers om trends te signaleren, onderhoudt contacten met beleidsmakers en verricht relevante literatuurstudies.

d 'Crisisbeheersing' is een defensief concept en wordt vaak gezien als een poging om de status quo te handhaven. Er werd gediscussieerd over de vraag of dit concept nog wel als denkkader volstaat of dat we eigenlijk een nieuw concept en een nieuwe term zouden moeten bedenken. Er werd geopperd dat 'resilience' of veerkracht wellicht een beter kader biedt dan crisisbeheersing.

e In de virtuele wereld bestaat er een sterke neiging om scheidingsmuren te slechten. Dit wordt 'de-perimeterisation' genoemd. Deze trend contrasteert sterk met ontwikkelingen in de fysieke wereld.

f In veel landen zijn middelen gereserveerd voor *forsight*. Om dubbel werk te voorkomen zou het verstandig zijn als landen op het punt van nationale veiligheid gaan samenwerken. Organisaties moeten echter worden betrokken bij de beoordeling van risico's en daar verantwoordelijk voor worden gemaakt, en wel zodanig dat er op basis van die beoordeling daadwerkelijk maatregelen worden getroffen. Een universeel toepasbare oplossing bestaat waarschijnlijk niet. Een gemengde benadering zou wel eens de beste oplossing kunnen zijn. Daar zouden zowel externe deskundigen als interne beleidsmakers bij moeten worden betrokken. Zo kan optimaal worden geprofiteerd van alle beschikbare informatie en kan tegelijkertijd de interne betrokkenheid bij en verantwoordelijkheid voor het proces worden gestimuleerd.

Samenvatting en slotconclusies

In zijn samenvatting gaf dagvoorzitter professor Michael Clarke drie hoofdthema's aan. Het eerste hoofdthema is de noodzaak, in crisissituaties, van een proces van identificatie, beoordeling en mobilisatie. Een tweede hoofdthema is dat de 'nieuwheidsfactor' zo veel mogelijk moet worden uitgeschakeld. Gebeurtenissen die ons verrassen zouden eigenlijk geen verrassingen mogen zijn. Het derde hoofdthema, ten slotte, is het creëren van de juiste politieke structuur. We moeten iemand de bevoegdheden geven om deze agenda daadwerkelijk vooruit te helpen. Zonder legitiem leiderschap zal het moeilijk zijn draagvlak te creëren voor een gezamenlijk doel.

Na de samenvatting door de voorzitter noemde Bruce Mann deze drie thema's nogmaals. Er waren met name twee aspecten die hij de deelnemers ter overweging wilde meegeven: de reis en de mensen.
Wat de reis betreft is het belangrijk om, ondanks eventuele nervositeit en angst voor het onbekende, onderscheid te maken tussen

- wat we tijdens de reis al begrijpen;
- inspanningen bovenop hetgeen we al hebben gedaan, of die we al eens eerder hebben gedaan maar dan buiten het terrein van de crisisbeheersing, en waar wij technieken kunnen aandragen;
- werkelijk nieuwe inspanningen (deze houden waarschijnlijk vooral verband met menselijke en sociale aspecten).

Het opzetten van samenwerkingsverbanden met mensen is bepaald geen radicaal nieuw uitgangspunt. Toch valt er nog veel te leren over de beste benadering. We moeten ons nadrukkelijker richten op de 'zachtere' termen en vaardigheden: relaties, vertrouwen, legitimiteit en empowerment. Volgens Bruce zijn deze concepten op zich dus niet nieuw, maar wel binnen de wereld van de crisisbeheersing, een tak van sport die inmiddels een buitengewoon breed terrein bestrijkt. Er zijn nu dan ook veel meer partijen waarvan we kunnen leren.

Er is behoefte aan uitbreiding van zowel instellingen als analytische hulpmiddelen. Die laatste bevinden zich vooral binnen het vertrouwde werkterrein van de instellingen en moeten meer worden gericht op gedragsanalyse. Ook de instellingen zelf moeten naar een hoger plan worden getild, vooral instellingen op het gebied van crisisbeheersing. Het gebrek aan grensoverschrijdende dialoog over risico's leidt echter tot frustratie.

Gezien de nieuwe inhoud en de grotere reikwijdte van het onderwerp is het niet langer mogelijk kwesties los van elkaar te beschouwen en moeten we het meer gaan hebben over institutionele samenwerking, ofwel partnerschap tussen instellingen, die alle bijdragen vanuit hun eigen vakgebied.

De weg voorwaarts

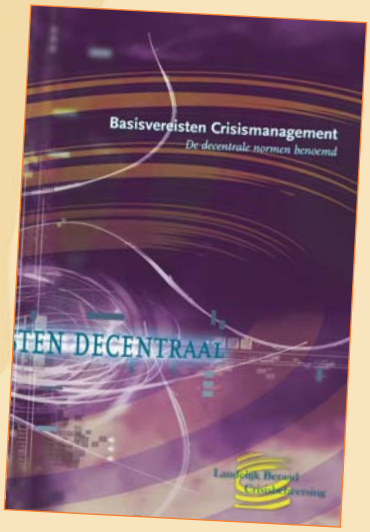
De deelnemers werd gevraagd zich te buigen over een aantal mogelijke resultaten van de conferentie.

1. Opzetten van een netwerk van mensen met interesse in hetzij brede kwesties hetzij specifieke aspecten daarvan. Dit zou kunnen leiden tot de ontwikkeling van een website.
2. Nog een dergelijke conferentie organiseren. Het VK wil dit met plezier op zich nemen, maar zou nog liever zien dat andere landen een aanbod doen.
3. Speciale evenementen organiseren rondom specifieke thema's, zoals:
   a. methodologie voor risicobeoordeling;
   b. communicatie over risico's en management van het publiek;
   c. *foresight* (op de langere termijn);
   d. bescherming van vitale infrastructuur;
   e. publiek/private partnerschappen;
   f. nationale strategieën voor crisisbeheersing.
4. Specifieke onderzoeksvoorstellen.

Reactie op de kanttekeningen van Boon en Helsloot

De basisvereisten crisismanagement in het juiste perspectief

In het februarinummer van dit magazine namen Bart Boon en Ira Helsloot de basisvereisten crisismanagement de maat. De basisvereisten zijn opgesteld door het Landelijk Beraad Crisisbeheersing op verzoek van de minister van BZK. Ze normeren de vier voorwaardenscheppende processen voor de rampenbestrijding en crisisbeheersing: melding en alarmering, opschaling, leiding en coördinatie en informatiemanagement. De minister van BZK wil deze eisen vastleggen in het Besluit veiligheidsregio's, waarvan het ontwerp nu ter consultatie in het veld ligt.



Boon en Helsloot bekijken hoe de basisvereisten van toepassing kunnen zijn bij verschillende typen situaties. Ze voeren drie verzonnen maar herkenbare scenario's op waarbij voor de zekerheid wordt opgeschaald tot GRIP-3. De conclusie die Boon en Helsloot trekken is helder. Ze stellen vast dat de vier processen bij verschillende typen rampen en crises verschillend ingevuld worden en dat het daarom moeilijk is om hiervoor kwantificeerbare normen te benoemen. Ze vinden dat de basisvereisten passen bij de symboliek van de alwetende en allesbepalende generaal die op basis van volledige informatie zijn troepen aanstuurt, gelijk de militaire doctrine uit de jaren tachtig. Dat beeld past volgens hen niet bij de werkelijkheid van crisisbeheersing en ook niet bij de huidige militaire inzichten. Zij waarschuwen voor de overtuiging dat het stellen van proceseisen zou volstaan of zelfs maar zin zou hebben.

Bij hun verwerping van proceseisen beroepen Boon en Helsloot zich op de Beethovenfout. Volgens de bedenker daarvan, primatoloog De Waal, is het verkeerd om te denken dat proces en product met elkaar overeenkomen. Twee dingen hierover. Ten eerste is de Beethovenfout hier helemaal niet van toepassing. Deze 'fout' heeft betrekking op het *spontane* proces van de evolutie en niet op door mensen ontworpen processen waar de basisvereisten over gaan.
Ten tweede is de Beethovenfout gebaseerd op een drogredenering. Natuurlijk is er een overeenkomst tussen proces en product. Ieder product is de uitkomst van een proces en ieder proces leidt tot een product. Als het product niet bevalt of het ziet er anders uit dan verwacht wil dat niet zeggen dat er geen relatie met het proces is. Het wil hooguit zeggen dat je het proces nog niet hebt doorzien, dat het verkeerd is ontworpen of dat het voortijdig is afgebroken.
Laten we met deze gedachte de kanttekeningen van Boon en Helsloot nog eens langslopen.

Melding en alarmering

Het doel van melding en alarmering is om de gehele crisisorganisatie snel en in haar geheel uit de startblokken te krijgen bij een acute ramp of crisis. Van de eisen hieraan doorstaan de eisen aan melding de toets der kritiek niet. Het LBCB stelde hier voor eisen te stellen aan de verwerkingscapaciteit van de meldkamer. Hoewel uit praktijktests is gebleken dat deze normen haalbaar zijn, is er voor gekozen om in het Besluit de uitkomst van het proces van melding te normeren: binnen een bepaalde tijd moet een beschrijving van het incident gereed zijn.

Opschaling

Boon en Helsloot stellen dat het principe van *one size fits all* voor de opschaling geen stand kan houden, want je hebt niet bij elk incident de hele hoofdstructuur nodig. Daar hebben ze gelijk in.
Het is hier van belang om nog eens duidelijk te maken wat het uitgangspunt van de basisvereisten ook weer was. Namelijk dat de hoofdstructuur van de crisisorganisatie

bij een acute ramp ineens kan opschalen tot GRIP-3. Het LBCB schrijft hierover in zijn rapport dat de basisvereisten vooral relevant zijn voor een acuut grootschalig incident, maar dat de normen in veel gevallen ook van toepassing kunnen zijn op voorzienbare incidenten of incidenten die zich langzaam ontwikkelen.
De gedachte achter het uitsluitend normeren van het optreden in de meest acute situatie, is dat als de veiligheidsregio's hun organisatie zo inrichten dat ze die situatie aankunnen, alle incidenten die een kleinere impact kennen ook afdoende bestreden kunnen worden. In het Besluit veiligheidsregio's blijft de mogelijkheid voor opschaling op maat nadrukkelijk open.
Boon en Helsloot vragen zich ook af waarom de basisvereisten alleen naar de opschaling van de leidinggevenden en hun staven kijken. Zij nemen aan dat hier wordt teruggevallen op een oude militaire doctrine die ervan uitgaat dat leidinggeven op afstand effect zou hebben. Een verkeerde aanname. Het was de opdracht voor het LBCB om nu juist de randvoorwaardelijke processen te normeren die bij iedere situatie van toepassing zijn. De inhoudelijke rampbestrijdingsprocessen worden al op andere plekken behandeld.
Het nut van het snel activeren van het operationeel team en de beleidsteams wordt ook in twijfel getrokken: voor het redden van mensen hebben ze geen betekenis en leiding geven op afstand heeft geen effect voor de resultaten op het rampterrein. Dat mag zo zijn, maar de teams hebben zo hun eigen taken vanaf de eerste fase. Twee voorbeelden daarvan zijn voorlichting door de burgemeester als "smoel" van de overheid naar de burger en het organiseren van bijstand door het operationeel team. Het is ook niet de bedoeling dat de teams de eenheden op het rampterrein direct aansturen, maar ze moeten voorwaardenscheppend bezig zijn en de crisispartners activeren.

Leiding en coördinatie

Boon en Helsloot wijzen het aangedragen besluitvormingsproces af. Ze zijn van mening dat het meer op een beleidsproces lijkt dan op crisisbesluitvorming. Zij vinden dat de gekozen uitgangspunten verkeerd zijn. Ze vinden dat het aankomt op de moed om snel te kunnen beslissen op basis van onvolledige informatie. Daarin hebben ze zonder meer gelijk, maar dat wil niet zeggen dat je dan niet de elementaire beginselen van besluitvorming zou moeten hanteren. Het gaat erom op basis van de beschikbare informatie de reëel mogelijke handelwijzen te onderkennen en een afweging te maken. Die afweging is belangrijk om fixatie op de meest voor de hand liggende oplossing en groupthink te voorkomen.
De normen die het LBCB aandroeg zijn op zichzelf waardevol als uitgangspunten om het proces van leiding en coördinatie te ontwerpen, maar de meeste bleken moeilijk in handhaafbare normen te vertalen. In het Besluit veiligheidsregio's vinden we ze dan ook niet terug. Wel wordt daar de basis van de crisismanagementcyclus vastgelegd.

Informatiemanagement

De uitwerking van de eisen aan het informatiemanagement in de basisvereisten komt volgens Boon en Helsloot neer op het verzamelen van alle informatie in een centraal punt, waar ze wordt gevalideerd, geanalyseerd en beoordeeld. Dit miskent volgens hen de essentie van crisisbesluitvorming.
Het uitgangspunt van het informatiemanagement in de basisvereisten is dat de juiste informatie in de juiste vorm en op het juiste moment beschikbaar is voor degenen die haar nodig heeft. De basisvereisten schrijven daarom voor dat de informatie eerst in het eigen beeld verwerkt moet worden en daarna gedeeld met andere direct belanghebbenden, voordat het in het centrale beeld terechtkomt. Dit sluit uitstekend aan bij de wens van Boon en Helsloot om de informatie zo snel mogelijk decentraal beschikbaar te stellen aan de 'frontlijnbeslissers', zoals de theorieën over *distributed decision making* voorschrijven. Maar de cirkel moet wel rondgemaakt worden: ook de hogere niveaus moeten zo goed mogelijk bediend worden om hun verantwoordelijkheid waar te kunnen maken. Die verantwoordelijkheid is niet die van een alwetende en allesbepalende generaal, maar van het hogere niveau dat een einddoel en randvoorwaarden bepaalt en het uitvoerende niveau dat *en detail* bepaalt hoe dat doel behaald wordt. Opdrachtgerichte commandovoering heet dat in de huidige militaire doctrine.

Proces of output? Allebei!

Boon en Helsloot zijn zeer kritisch over de basisvereisten en ze bepleiten in plaats daarvan het wettelijk vastleggen van eisen aan de output van de rampbestrijdingsorganisatie. Zij menen dat die output te kwantificeren is in termen van gekwalificeerde mankracht op de plekken waar de hulpverleners moeten werken bij een ramp of crisis. Dat laatste is een goede analyse en daar moet iets mee gebeuren. Maar om de juiste mensen in de juiste hoeveelheden op de juiste plek te krijgen en ze de juiste dingen te laten doen, moeten die mensen wel weten dat ze in actie moeten komen (alarmering en opschaling), wat er aan de hand is (informatievoorziening) en moeten ze ook aangestuurd en ondersteund worden (leiding en coördinatie). Dat zijn precies de zaken die in de basisvereisten geregeld worden.

Erik Klaver,
senior beleidsmedewerker directoraat-generaal Veiligheid, Programma Veiligheidsregio's, ministerie van BZK (erik.klaver@minbzk.nl)

Outputeisen stellen minder simpel dan het lijkt

Reactie op kanttekeningen basisvereisten

De grote lijn van het artikel

Bart Boon en Ira Helsloot trekken de praktijkwaarde in twijfel van de basisvereisten voor het crisismanagement van het LBCB. Zij beginnen met te onderschrijven dat crisismanagement 'de bottleneck vormt voor het optreden van de hulpverleningsdiensten'. Ze ronden af met het voorstel om, in plaats van eisen aan het crisismanagement, 'de output van de rampenbestrijding in een wettelijke eis neer te leggen'. Je denkt dan meteen aan de *Leidraad operationele prestaties* uit 2001, een lijvig boekwerk met concrete resultaten per bestrijdingsproces. Maar gelukkig hebben de auteurs voor het *kwantificeren* van de echte output een veel eenvoudiger criterium, namelijk 'de aanwezigheid van gekwalificeerde menskracht op de verschillende locaties'. Maar was dat niet input? Is niet juist bij diverse incidenten gebleken dat ondanks de aanwezigheid van allerlei zeer gekwalificeerde mensen er elementaire zaken mislopen? En hoe krijg je de juiste menskracht op tijd op de juiste locaties? En hoe creëer je goede werkcondities voor hen? Kom je dan niet weer uit bij het crisismanagement dat – dan nog steeds – de bottleneck vormt voor het optreden van die menskracht? En waren de eisen aan dat crisismanagement niet juist door het veld zelf opgesteld?

Andere misverstanden

Ook op andere punten kan het artikel de mensen, die nu met veel inzet werken aan het verbeteren van het crisismanagement, op het verkeerde been zetten.
Het LBCB heeft een realistische minimumeis gesteld aan het registreren van essentiële gegevens uit meldingen. Verontrustend is dat de auteurs zich afvragen wat de waarde is van het vastleggen van gegevens in GMS. Zoals bekend delen de centralisten daarmee de informatie met elkaar en wordt voorkomen dat essentiële gegevens in de hectiek uit beeld raken. Vanuit het GMS kan snel een beeld van de ramp worden samengesteld. Bij elke ramp en simulatie blijkt hoe cruciaal deze gegevens zijn voor de alarmering, opschaling en bestrijding.
De auteurs stellen dat het operationeel team en de beleidsteams in de eerste twee uren niet van belang zijn voor het aantal slachtoffers dat gered kan worden. Kennelijk veronderstellen de auteurs dat in de omgeving van het rampterrein (die valt onder het ROT) zoals bij een gifwolk geen mensen hoeven te worden gered. Uit rampenonderzoek blijkt juist dat sturing en ondersteuning vanuit een ROT cruciaal kan zijn om voldoende capaciteit voor redding en geneeskundige hulpverlening op de juiste plaatsen te krijgen via begidsen, vrijhouden van toegangsroutes et cetera. Ook zijn leidinggevenden van het ROT en de burgemeester of voorzitter van de veiligheidsregio meteen na alarmeren al beschikbaar om zonodig 'knopen door te hakken'. Dat alles natuurlijk op basis van een juist en actueel beeld van de situatie. Daar heb je weer het ROT voor nodig. Volgens de basisvereisten zal het hoofd van de sectie Informatiemanagement al binnen 30 minuten na alarmering starten met zijn werk en de volledige sectie binnen 40 minuten. Zou op dat moment een actueel beeld en overzicht van de ramp, de knelpunten en de nog ontbrekende gegevens niet ook van belang zijn voor de professionals op het rampterrein?

De auteurs stellen verder dat in de realiteit van crisisbeheersing er 'vaak geen mogelijkheid is tot monitoring, laat staan bijstelling van acties'. Dat wekt de suggestie dat men maar moet blijven doorgaan met een gekozen en inmiddels zinloos geworden aanpak. De basisvereisten, met als kern een goede informatiepositie, zijn er juist op gericht om pro-actief en flexibel te reageren op nieuwe feiten. De *State of the art 2007* van het LBCB over bestuurlijk leiderschap in crisissituaties bevat in dit kader een cruciale passage: 'In onzekere situaties heeft ieder mens een fundamentele voorkeur voor informatie die een bestaand beeld bevestigt in plaats van informatie die dit beeld verwerpt of ontkracht. In teamverband kan op deze wijze een situatie ontstaan waarin iedereen elkaar naar de mond praat, omdat hierdoor de onzekerheid afneemt over wat er aan de hand is. Dit verschijnsel, dat ook wel *group think* wordt genoemd, moet volgens bestuurders worden voorkomen, omdat het desastreuze gevolgen kan hebben voor de besluitvorming.'

Slot

De rampenbestrijding moet einde 2009 op orde zijn.
Ik zie dit op grond van de ervaring uit doorlichtingen en incidentonderzoek en doorlichtingen als ambitieus, maar noodzakelijk en haalbaar. Eenheid van opvatting over het wat en hoe is dan een eerste vereiste. De redenering en genoemde stellingen van beide auteurs dragen daar niet aan bij.

Simon van der Doorn,
procesmanager Toezicht Inspectie OOV

Besluit Veiligheidsregio's in consultatie

Deze maand worden verschillende koepels in het veiligheidsveld gevraagd om een reactie te geven op het Besluit Veiligheidsregio's, de zogenaamde kwaliteits-AMvB. Dit besluit is gebaseerd op de Wet veiligheidsregio's. In het besluit worden eisen gesteld aan de organisatie en taken van de regio's en de brandweerzorg. Minister Ter Horst heeft het besluit ter consultatie naar het veld gestuurd met het verzoek om in mei 2008 te laten weten wat zij van het besluit vinden. De consultatie richt zich vooral op bestuurders zoals vertegenwoordigd in het Veiligheidsberaad, de VNG en het IPO met het verzoek ook de reacties van de koepels van de professionele beroepsgroepen mee te nemen in hun reactie.

Waarom dit besluit?

In het besluit wordt het basisniveau beschreven waar alle regio's over twee jaar aan moeten voldoen en waar alle burgers in Nederland op kunnen rekenen. De meer concrete doelstelling is het verzorgen van uniformiteit in de organisatie en de prestaties van de regio´s. Dit is van belang voor het mogelijk maken van interregionale bijstand en bovenregionaal optreden.
Het besluit bevat voor een deel regelgeving die op dit moment ook al in besluiten vastligt. Het gaat om het Besluit bedrijfsbrandweer, het besluit over categorieën inrichtingen en luchthavens aanwijzen voor een rampbestrijdingsplan en de BDUR. Voor een ander deel bevat dit besluit nieuwe regelgeving. In het besluit zijn geen kwaliteitseisen aan het personeel van brandweer, meldkamer en GHOR opgenomen. Dit komt in een andere AMvB die een eigen tijdpad kent.

Organisatie van de rampenbestrijding en crisisbeheersing

In het hoofdstuk over de organisatie van de rampenbestrijding wordt de hoofdstructuur van de crisisorganisatie vastgelegd. In de meeste regio's is de hoofdstructuur al bekend. Hij is gebaseerd op het referentiekader GRIP. Dit hoofdstuk bevat ook eisen aan de processen die kritisch zijn voor het slagen van het crisismanagement om ervoor te zorgen dat de crisisorganisatie van de regio vlot en in zijn geheel uit de startblokken kan komen bij een acute ramp of crisis. Het idee is dat als de regio dit zwaarste scenario aankan, alle incidenten met een mindere impact ook goed bestreden worden. Opschaling op maat blijft dus mogelijk.
De brandweer speelt een centrale rol bij in de veiligheidsregio. In het besluit is daarom geregeld hoe een basisbrandweereenheid is samengesteld en wat de opkomsttijden voor verschillende typen objecten zijn. Voor bijvoorbeeld een bejaardenhuis geldt straks een opkomsttijd van 5 minuten maar bij een autobrand is het voldoende dat de brandweer binnen 15 minuten arriveert. De normen zijn afgeleid van bestaande leidraden en handboeken.

Ongevalsbestrijding gevaarlijke stoffen

In hoofdstuk 4 is de ongevalsbestrijding gevaarlijke stoffen genormeerd. De samenstelling van de bestrijdingseenheden wordt beschreven, de taken van deze eenheden verder uitgewerkt en ook hier gelden enkele tijdseisen aan prestaties. Bij deze prestaties moet gedacht worden aan opkomsttijden, het verrichten van metingen en het uitbrengen van een advies. Deze normen komen uit de leidraad Officier Gevaarlijke Stoffen (OGS).

Afspraken tussen de GHOR en zorginstellingen

Om invulling te geven aan hun verantwoordelijkheid op het gebied van geneeskundige hulpverlening bij ongevallen en rampen moet het bestuur van de veiligheidsregio schriftelijke afspraken maken met de zorgaanbieders in de regio, bijvoorbeeld ziekenhuizen en ambulancediensten. De afspraken gaan over de procedures tijdens rampen en crisis en het gezamenlijk opleiden en oefenen.

Michiel Verlaan, beleidsmedewerker, Programma Veiligheidsregio, ministerie van BZK

Het ontwerp Besluit veiligheidsregio's is te downloaden via **www.minbzk.nl/veiligheidsregio**.

Naschrift op repliek Basisvereisten crisismanagement

De kern van wetenschap is het wetenschappelijk debat. Erik Klaver riposteert vanuit dat perspectief fraai op onze eerdere bijdrage met twijfels over de basisvereisten van het LBCB. Natuurlijk kunnen wij het niet nalaten te wijzen op het feit dat, gelukkig, het ministerie de basisvereisten waaraan wij het meeste morrelden niet heeft opgenomen in de consultatieversie van de kwaliteits amvb. Voor een aantal van de andere punten geldt dat de precieze definities die wij hanteren blijkbaar verschillen, een argument te meer voor meer inspanning gericht op wetenschappelijke fundering van het crisisbeheersingsbeleid.
De reactie van Simon van der Doorn kunnen wij ook alleen maar lezen als wijzend op de noodzaak van meer wetenschap en vooral meer kennis van de praktijk. Gedeelde kennis is noodzakelijk voordat gekomen kan worden tot 'de vereiste eenheid van opvatting'.

Ira Helsloot en Bart Boon

Resultaten Denk Vooruit campagne leiden tot nieuwe strategie

Groot bereik, goede waardering, geringe gedragsverandering

Op 18 februari jl. berichtten diverse media (RTL, Volkskrant, AVRO) over tegenvallende resultaten van de Denk Vooruit campagne. Deze campagne, gestart in september 2006, heeft als doel om burgers te informeren over de risico's in hun woon- en leefomgeving, hoe zij zich op deze risico's kunnen voorbereiden en om hun zelfredzaamheid tijdens een ramp of crisis te verhogen. Bij de campagne zijn radio- en TV-spots ingezet, is een website ingericht en zijn middelen beschikbaar gesteld aan gemeenten. In totaal zijn elf ramptypen uitgewerkt. Doelgroep van de campagne: alle inwoners van Nederland van 13 jaar en ouder. Het Expertisecentrum Risico- en Crisiscommunicatie (ERC) leidt deze campagne.

DENK VOORUIT

Feitelijke campagneresultaten

Na 1,5 jaar campagnevoeren (najaar 2006 tot heden) leveren de effectmetingen van de Rijksvoorlichtingsdienst het volgende op:

- De campagne heeft 91% van de Nederlanders van 18 jaar en ouder bereikt (91% heeft minimaal een van de uitingen gezien). Dit ligt boven de algemene benchmark van Postbus 51 campagnes, het gemiddelde van alle overheidscampagnes. Dat is namelijk 89%.
- De waardering van de campagne is gemiddeld tot goed (rapportcijfer 6,6 is op de benchmark). De banner krijgt het rapportcijfer 6,9 (benchmark = 6,2);
- Meer dan de helft (58%) zegt spontaan dat de belangrijkste boodschap van de campagne is dat 'je jezelf moet voorbereiden op een ramp'.

Gedragsverandering

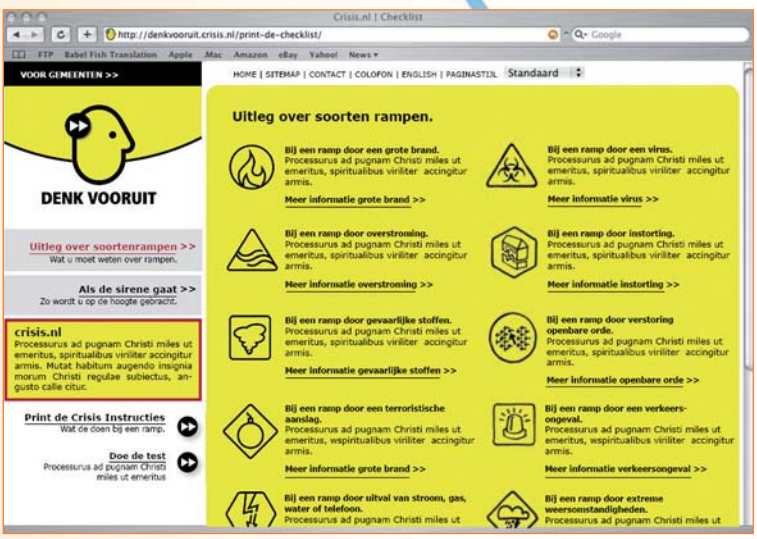
Vanuit hetzelfde onderzoek concludeert het ERC verder dat mensen het belangrijk vinden dat er campagne wordt gevoerd: mensen willen geïnformeerd worden door de overheid over risico's. Sinds september 2006 heeft een kleine 600.000 unieke bezoekers de campagnesite **www.denkvooruit.nl** bezocht. Ook blijkt dat 54% van de mensen de regionale rampenzender heeft ingesteld. De behoefte aan informatie is er. De intentie om vervolgens echt voorbereidingsgedrag te vertonen is er ook ('Ik vind dat ik eigenlijk wel een zaklamp en een radio op batterijen zou moeten aanschaffen"), maar het feitelijk gedrag, het aanschaffen van die middelen of het in huis hebben van een noodvoorraad, blijft achter.

Dit is een herkenbaar beeld bij campagnes die gedragsverandering tot doel hebben. De crux bij voorlichting over risico's is dat mensen in Nederland zich niet kunnen voorstellen dat er een ramp gebeurt. Negen op de tien mensen voelen zich veilig in de eigen leefomgeving. De urgentie wordt (nog) niet gevoeld om zich daadwerkelijk voor te gaan bereiden. Het blijft bij intenties. Ira Helsloot, hoogleraar crisisbeheersing en fysieke veiligheid in Amsterdam, beaamde dit in zijn commentaar in o.a. de Volkskrant: 'Uit wereldwijd wetenschappelijk onderzoek is al vaak gebleken dat dit soort campagnes niet werkt. Mensen maken een rationele afweging: de kans op een ramp is zo klein, dat ze zich daar niet tegen in gaan dekken."

Rol gemeenten

Kernpunt bij de Denk Vooruit campagne is dat op nationaal niveau slechts algemene boodschappen in massamediale middelen kunnen worden verwerkt. Het geven van concrete, op maat gemaakte informatie, is vooral de taak van gemeenten. Dat verwachten burgers ook. Tot nu toe hebben niet alle gemeenten hun rol in de campagne (optimaal) ingevuld. Tweederde van de gemeenten doet actief mee om de campagne een lokale invulling te geven,

dat wil zeggen gemeentelijke informatie is terug te vinden na het intypen van je postcode op **www.crisis.nl/gemeenten** of drukwerk is aangevuld met gemeentelijke contactgegevens en frequenties van de regionale calamiteitenzender. Een aantal gemeenten heeft de campagne-uitingen volledig in de eigen gemeentelijke of regionale risicocommunicatie verwerkt. Campagne-inspanningen voor de komende jaren moeten er op gericht zijn gemeenten op indringender manier te wijzen op hun wettelijke verplichtingen aangaande risicocommunicatie en hen daarbij optimaal te faciliteren.
Zo subsidieert het ministerie van BZK onder andere een beperkt aantal regionale en lokale initiatieven met als voorwaarde dat de ontwikkelde instrumenten door andere gemeenten en regio's gebruikt kunnen worden.



Zelfredzaamheid bij burgers

Minister ter Horst van BZK gaf in een toespraak tijdens het veiligheidscongres in november 2007 aan dat 'we in onze risicosamenleving niet van de overheid mogen verwachten dat ze als enige optreedt en dat de burgers afwachtend zijn. Als elke seconde telt is juist de inzet van burgers van groot belang'. Met de wetenschap dat BZK meer moet koersen op (zelf)redzaamheid ontstaat een nieuwe werkelijkheid; burgers, bedrijfsleven en hulpverleningsorganisaties moeten worden voorbereid op hun nieuwe verantwoordelijkheid.

De resultaten van de Bobcampagne zijn niet enkel geslaagd vanwege een succesvolle voorlichting. Er zijn drie instrumenten te gebruiken om te beïnvloeden, ook wel zweep, peen en preek genoemd. Onder 'peen' worden bijvoorbeeld subsidies verstaan. De 'preek' is de voorlichting en de 'zweep' betreft sancties, accijns, bekeuringen, controle-instrumenten. Wanneer de communicatie hand in hand gaat met de inzet van andere beleidsinstrumenten kan er meer effect behaald worden.

Meerjarenstrategie

BZK bezint zich momenteel op een vervolgstrategie voor het bevorderen van zelfredzaamheid voor de komende jaren. Hierin worden concrete beleidsdoelstellingen en beleidsinstrumenten uitgewerkt. Aansluitend wordt ook de campagnestrategie voor Denk Vooruit nieuw leven ingeblazen. Wie willen we bereiken, met welke boodschap en welk doel en hoe kunnen we de gemeenten/veiligheidsregio's hierin betrekken?

Reactie minister BZK

De minister meent naar aanleiding van de krantenartikelen dat de rampencampagne Denk Vooruit aanmerkelijke bijstelling nodig heeft. Zij vindt – analoog aan de ontwikkeling van de meerjarenstrategie – dat bij de uitvoering van de campagne meer geredeneerd moet worden vanuit het gedrag van de burger. Een steviger boodschap is dan ook nodig. Burgers moeten ervan doordrongen raken, dat men zich zo moet voorbereiden dat men de eerste drie dagen van de ramp zelfredzaam is, omdat de overheid niet altijd beschikbaar is. Een dergelijke rationele boodschap wordt in de Verenigde Staten en Canada aan de bevolking meegegeven. De burger dient vanuit de aangereikte kennis zo gestimuleerd te worden dat hij/zij de indringende campagneboodschap aannemelijk vindt en het voor de hand vindt liggen bijvoorbeeld een noodvoorraad aan te leggen. Zoals eerder aangegeven is het menselijk gedrag niet alleen met communicatie te veranderen. Wet- en regelgeving en een strakker sanctiebeleid leiden er eerder toe dat mensen het juiste gedrag gaan vertonen. Voorop staat uiteindelijk dat burgers een ramp of crisis weten te overleven door de handelingsperspectieven die de overheid via TV- en radiocommercials, de website **crisis.nl** plus de brochure en de rampeninstructiekaart aanreikt.

Frank Vergeer,
projectleider Denk Vooruit
Roos Lamers,
projectmedewerker rampencampagne en redacteur risicoencrisis.nl
Anja van den Bosch-Overduin,
beleidsmedewerker, Expertisecentrum Risico- en Crisiscommunicatie (ERC)

Internationale opslag van landbouwzaden op Spitsbergen

Op 25 februari werd de internationale opslagfaciliteit voor land- en tuinbouwzaden op de Noorse eilandengroep Spitsbergen, de Svalbard Seed Vault, geopend. Deze in de permafrost gelegen faciliteit biedt een veiligheidsgarantie voor onze wereldwijde voedselvoorziening.

De oorsprong van de landbouw

Landbouw, het "domesticeren" van planten en dieren, begon ongeveer 10.000 jaar geleden. Jagers werden veehouders en verzamelaars werden boeren. Maar niet overal tegelijkertijd. Bepaalde gebieden in de wereld herbergden een geschikte combinatie aan planten en dieren om de overstap naar landbouw mogelijk te maken, en waarschijnlijk gaven klimaatswijzigingen het benodigde duwtje. Waar landbouw ontstond, ontwikkelde zich een vrijgestelde klasse, en die leidde tot sterke cultuurontwikkeling. Zo kwamen tarwe en gerst, erwten en veldbonen, rundvee en geiten uit het Midden-Oosten, rijst en soja, kippen en varkens uit Zuidoost Azië, en maïs, bonen en kalkoen uit Mexico, in directe samenhang met de Mesopotamische, Chinese en Maya culturen.

Variatie en erosie

Boeren pasten de planten en dieren aan aan hun wensen, en wanneer ze migreerden of materiaal ver weg verkochten, pasten gewassen en landbouwhuisdieren zich noodgedwongen aan de nieuwe omstandigheden aan. Zo ontstond steeds meer variatie binnen de gewassen en landbouwhuisdieren. Kool, bloemkool, broccoli, spruitjes en koolrabi behoren allemaal tot de zelfde biologische soort. In Nederland had elk dorp zijn eigen appelras, en kennen we veel regiogebonden landbouwhuisdierrassen zoals Groninger Blaarkop, Texelse schapen, en het Chaams hoen.
Maar veel van die variatie is weer (bijna) verdwenen. Oorzaak daarvan is de industrialisatie van onze land- en tuinbouw: de rol van boeren als selecteurs is al weer lang geleden overgenomen door professionele fokkers en veredelaars, terwijl mechanisatie in de landbouw en de marktwerking in de detailhandel om uniforme producten vragen. Ook de globalisering leidt tot eenheidsworst, steeds meer zien we dezelfde voedselpatronen overal ter wereld, met McDonalds als bekendste voorbeeld. Diversiteit is uit het gezicht verdwenen, en veel oorspronkelijke diversiteit is zelfs uitgestorven. Dat verschijnsel is bekend als genetische erosie. En genetische erosie vormt een probleem.

Wereldvoedselzekerheid en duurzame productie

Om ook in de toekomst de wereldbevolking te kunnen blijven voeden, moeten we de opbrengst verhogen, maar ook reageren op nieuwe ziekten en plagen en onze voedselproductie aanpassen aan de komende klimaatverandering. Deze klimaatverandering zal tot aanzienlijke verdroging van bepaalde gebieden leiden, bijvoorbeeld Zuidelijk Afrika en het Middellandse Zeegebied, terwijl in andere gebieden de temperatuur te hoog wordt voor onze huidige gewassen, bijvoorbeeld in India en Zuidoost-Azië. Ook consumentenwensen veranderen. Zo is er nu weer meer belangstelling voor uitgesproken smaken en variatie op ons bord dan de afgelopen decennia. Denk bijvoorbeeld aan de toenmalige kritiek op de Nederlandse tomaat ("Wasserbombe") en de variatie aan tomaten die nu weer in de supermarkt te vinden is. Ook stelt een duurzamer productie eisen aan de planten en dieren die we gebruiken, in de vorm van een efficiëntere benutting van water, meststoffen en diervoeders. Om een antwoord te kunnen vinden op al deze huidige en toekomstige eisen is blijvende beschikbaarheid van genetische variatie een vereiste. In de

veelheid van rassen en herkomsten zit namelijk een enorme diversiteit verborgen.

Genenbanken

Vooral in de jaren zeventig en tachtig van de vorige eeuw zijn daarom genenbanken in het leven geroepen. Instellingen die als taak hebben om de genetische variatie in onze gedomesticeerde planten en dieren zo goed mogelijk te bewaren. Ook het Centrum voor Genetische Bronnen Nederland (CGN) stamt uit die tijd. Het werd in 1985 opgericht voor het opbouwen van collecties van genetisch uitgangsmateriaal van voor Nederland belangrijke gewassen en landbouwhuisdieren. In Wageningen wordt het materiaal, zoals in de meeste genenbanken, gedroogd en bij lage temperatuur (-18 °C) bewaard. De collecties bevatten veel materiaal dat in de tientallen jaren daarvoor al in Wageningen verzameld was, aangevuld met materiaal uit eigen buitenlandse verzamelmissies. Deze collecties vertegenwoordigen een niet te becijferen waarde voor de toekomstige wereldvoedselzekerheid en een meer duurzame landbouw.
Maar met de oprichting van genenbanken is de genetische erosie niet ten einde gekomen. Vooral in ontwikkelingslanden komt het voor dat genenbanken onvoldoende financiële middelen hebben om de zaden goed in stand te houden en het materiaal opnieuw te vermeerderen als dat nodig blijkt. Met andere woorden, in zo'n geval zet de genetische erosie zich in de genenbanken voort. Gelukkig is dat in Wageningen niet het geval dankzij de subsidie van het ministerie van LNV. Maar er loeren ook andere gevaren: brand kan de collecties vernietigen en ook door langer durende stroomuitval kunnen ze beschadigd worden. Tenslotte zou ook een overstroming van de Rijn bij Wageningen tot verlies van de collecties kunnen leiden. Daarom wordt het Wagenings collectiemateriaal ook elders in Europa opgeslagen. Maar wie kan er 100 jaar vooruit kijken en de politieke situatie dan voorspellen? Zo is de idee voor een nog veiliger wereldopslagplaats geboren.

Waarom Spitsbergen?

De Svalbard Seed Vault biedt zo'n veilige opslagfaciliteit om twee hoofdredenen: klimatologisch en politiek-strategisch. De Seed Vault bestaat uit een nieuw in de berg uitgehakte lange gang van 120 meter die uitkomt op drie gewelven van 27 bij 10 bij 6 meter, die gezamenlijk ruimte bieden aan 4.5 miljoen zaadmonsters. De gewelven worden net zoals de opslagruimten in Wageningen op -18 °C gehouden. Maar de Svalbard Seed Vault biedt meer.
Als in Spitsbergen de stroom uitvalt, fungeert de berg als een gigantische isolator. Aangezien in de berg permafrost condities heersen, blijft de temperatuur beneden nul, de belangrijkste voorwaarde voor het goed blijven van het zaad. Daarnaast ligt Spitsbergen ver van de bewoonde

wereld. Als er elders ter wereld politieke conflicten uitbreken is het onwaarschijnlijk dat deze Spitsbergen raken. Tenslotte geldt dat de regering van Noorwegen, die de faciliteit voor 6 miljoen euro heeft laten aanleggen, als een van de weinige landen ter wereld acceptabel en betrouwbaar is voor ontwikkelde landen en ontwikkelingslanden. Veel landen zien hun genetisch uitgangsmateriaal namelijk als een belangrijke economische asset. De Noorse regering regelt in het contract met de afzender dat deze eigenaar van het materiaal blijft en als enige over de bestemming kan beslissen.

Het begin is er

Bij de opening van de Svalbard Seed Vault waren er al 400.000 monsters van twintig verschillende partijen aangekomen en opgeslagen. Daarbij waren ook 18.000 monsters van het CGN uit Nederland, ongeveer driekwart van de totale collectie. Het betreft zaden van uiteenlopende gewassen zoals sla, ui, kool, aardappel, tomaat, paprika, komkommer, tarwe en gerst, om een aantal belangrijke te noemen. De andere collecties die als in Svalbard zijn gearriveerd zijn vooral afkomstig van de internationale landbouwonderzoekinstellingen en bevatten alle belangrijke voedselgewassen, zoals tarwe, rijst, maïs, aardappel en bonen. De verwachting is dat de voorraad in Svalbard snel verder zal toenemen en binnen korte termijn inderdaad de variatie van alle wereldvoedselgewassen zal veilig stellen.

Bert Visser,
directeur Centrum voor Genetische Bronnen Nederland

Waar beveiliging het hardst nodig is, verdient beleid aanscherping

Tegenwoordig is het mogelijk om je zaken altijd en overal online te regelen en dus floreert de e-commerce in Nederland als nooit te voren. Webwinkels schieten in 2007 als paddenstoelen uit de grond en het online winkelen mag zich verheugen in een explosief stijgende populariteit. Ook bedrijven en overheidsorganisaties maken de afgelopen jaren steeds meer gebruik van internet als portaal naar hun klant. Deze tendens brengt echter ook een aantal ernstige risico's met zich mee. Risico's waar vooral de overheid zich vaak onvoldoende van bewust is. Wat te denken van het gevaar van internetfraude, als gevolg van phishing en hacking, en het risico dat een groot deel van onze gevoelige overheidsinformatie op straat komt te liggen?

Organisaties kunnen het zich niet veroorloven dat financiële gegevens en klantgegevens kwijtraken of dat derden met persoonlijke informatie op de loop gaan. Toch blijkt uit het ICT Barometeronderzoek van Ernst & Young[1] dat maar vier op de tien organisaties over een noodplan beschikken wanneer het kritische bedrijfsproces wordt gehackt, uitvalt of niet meer goed functioneert. Binnen de (semi-)overheidssector is dit zelfs nog lager: hier beschikt maar een kwart over een noodplan. Een schrikbarende zaak als je je realiseert dat een groot deel van de Nederlandse organisaties enorm, zoniet volledig, afhankelijk is van ICT. Daarbij geldt: hoe groter en dienstverlenender het bedrijf, hoe groter de afhankelijkheid. Tel daarbij op dat bijna de helft van de bedrijven regelmatig – in meer of mindere mate – te kampen heeft met ernstige cybercrime, en je kunt niet anders dan concluderen dat een noodplan simpelweg een dwingende prioriteit is. Juist daar waar beveiliging tegen computercriminaliteit het hardst nodig is, dient het beleid te worden aangescherpt. In de praktijk blijkt dat de risico's hand over hand toenemen. De tijd om hier onverschillig over te kunnen zijn, is echt voorbij. We staan anders aan de vooravond van grote digitale narigheid en iedereen moet wakker geschud worden. Dit is noodzaak willen we tijdig en adequaat kunnen reageren op digitale aanvallen die grote gevolgen hebben voor de samenleving.

Beveiligingsbewustwording

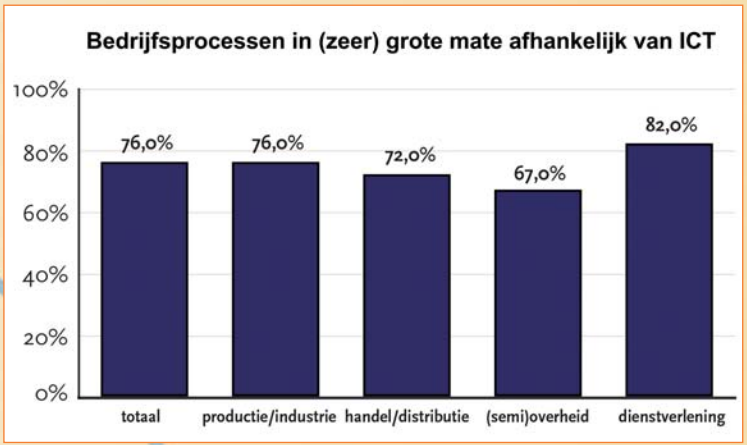
Inderdaad vragen deskundigen zich overal ter wereld af of veilig internetten nog wel mogelijk is. Want hoewel het aantal virussen en hackpogingen lijkt te dalen, worden de gevolgen steeds groter. Niet alleen treedt er gewenning op tegen cybercrime, de *cybercriminals* worden ook steeds professioneler en zijn steeds vaker internationaal actief. Wanneer er daadwerkelijk cybercrime plaatsvindt, is de schade daardoor veel groter.
Toch zijn het juist de geënquêteerde overheidsmanagers die maar weinig geïnteresseerd lijken in cybercrime en daardoor mogelijk niet goed voorbereid zijn. De beveiliging van hun systemen laat, naar eigen zeggen, te wensen over en uit het ontbreken van noodplannen blijkt duidelijk dat de (semi) overheden hun afhankelijkheid van de ICT zwaar onderschatten. Terwijl hun systemen over het algemeen veel meer kritische informatie bevatten dan die van de meeste overige Nederlandse bedrijven en dienstverleners. Gevraagd naar het vertrouwen in de veiligheidsmaatregelen tegen cybercrime, geeft maar een kleine 38 procent overheidsmedewerkers aan dat ze vertrouwen op de beveiligingsmaatregelen van hun werkgever. Aanmerkelijk lager dan binnen het bedrijfsleven, waar meer dan de helft het volste vertrouwen heeft in de werkgever.

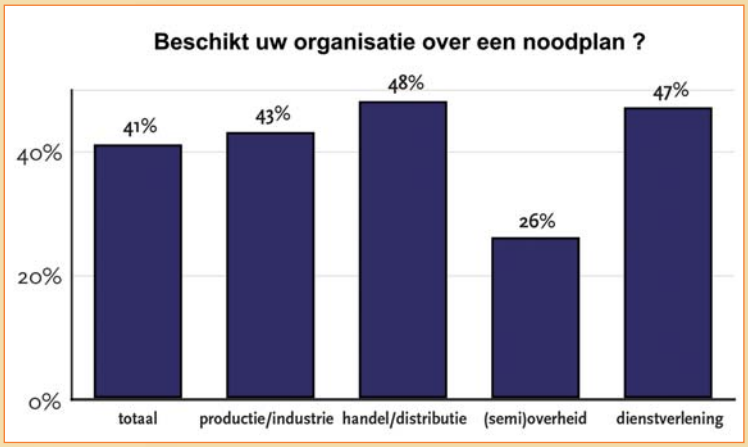
Bijna alle organisaties hebben wel technische maatregelen getroffen om de schade door cybercrime te voorkomen. De meest toegepaste maatregelen zijn firewalls, anti-virus software en anti-spywaresoftware. Hoewel dit soort technische beveiliging natuurlijk onmisbaar is, lossen ze maar een deel van het probleem op. Een groot deel van het probleem wordt namelijk ook veroorzaakt door het ontbreken van organisatorische maatregelen. Bijvoorbeeld heldere afspraken over veilige werkprocessen of over wat medewerkers wel of niet via internet mogen doen. Gelukkig proberen steeds meer organisaties om hun medewerkers 'beveiligingsbewust' te maken, voornamelijk door het geven van voorlichting.

Heeft aangifte zin?

Wat doen bedrijven als ze zijn gehackt of last hebben van andere vormen van cybercrime? In de praktijk bar weinig, zo blijkt uit de ICT Barometer. In de meeste gevallen doen bedrijven die een cybercrime aanval te verduren hebben gehad, namelijk geen aangifte bij politie of justitie. Twee op de tien bedrijven ondernemen zelfs helemaal geen

[1] *Uitgevoerd onder een representatieve groep van ruim 600 managers en leidinggevenden bij de Nederlandse overheid en in het bedrijfsleven.*





actie waarbinnen dit bij kleine bedrijven (tot 20 werknemers) zelfs in vier op de tien gevallen zo is. De meeste bedrijven die wel iets doen, houden hun onderzoek in eigen beheer. Simpel, omdat ze niet overtuigd zijn dat aangifte doen zin heeft. Een aantal bedrijven heeft zelfs geen idee wáár ze moeten zijn voor aangifte. Ook hieruit blijkt dat we het in Nederland niet goed voor elkaar hebben. Burgers moeten betere informatie krijgen en hun vertrouwen moet herwonnen worden.
De onlangs gehackte OV-chipkaart draagt aan het laatste zeker niet bij. Ook een situatie als in Engeland in oktober 2007, waar de gevoelige informatie van 25 miljoen burgers door een fout van de overheid zoek raakte, is in Nederland een reële dreiging. Tel daar nog bij op dat in principe alle informatie bij de overheid openbaar is, dus ook informatie over slecht functionerende ICT, of het zoekraken van gevoelige informatie. Wat nodig is, is een alerte overheid die zorgt dat het ICT (beveiliging) beleid niet versnipperd wordt uitgevoerd.

Vervolging en bestrijding

Conclusie? Digitaal Nederland moet veiliger. Het is dan ook goed nieuws dat de regering cybercrime intensiever wil gaan bestrijden.Cybercrime is een van de speerpunten van ons kabinet, en daarbij hoort een programma voor de aanpak van cybercrime. Voor 2008, maar ook voor daarna. Het programma voorziet onder andere in een intensievere bestrijding van cybercrime door opsporing en vervolging, in voorlichting voor burgers en ondernemingen en in het tegengaan van extreme uitingen in elektronische netwerken. Een belangrijk onderdeel is ook het *landelijke meldpunt Cybercrime*. Een initiatief van de ministeries van Justitie en Binnenlandse Zaken, waarbij het Korps Landelijke Politie Diensten verantwoordelijk is voor het doorzetten van de *meldingen* naar het juiste loket. Let wel, het gaat hierbij om meldingen en niet om aangiften. Voor aangiften moeten bedrijven en organisaties nog steeds contact opnemen met het plaatselijke politiebureau.

Het ICT Barometeronderzoek van Ernst&Young werd gehouden onder 600 leidinggevenden van de Nederlandse overheid en het bedrijfsleven.

De onderzoeksresultaten kunnen worden opgehaald op **www.ictbarometer.nl.**

Jacob Verschuur,
director Ernst & Young ICT Leadership en verantwoordelijk voor Trends in ICT en ICT Barometer
Monique Otten,
partner Ernst & Young EDP Audit

Cybercrime?

Bij Cybercrime gaat het om criminele activiteiten waarbij de computer of het netwerk een belangrijk onderdeel uitmaakt. Denk bijvoorbeeld aan internetfraude, hacken, social engineering of spam. Het verschil tussen een hacker en een social engineer is dat hackers toegang proberen te krijgen tot systemen door gebruik te maken van kwetsbaarheden in die systemen. Een social engineer richt zich het kwetsbaarste onderdeel van de beveiligingsketen: de mens áchter de pc. Dat doet hij bijvoorbeeld door gebruik te maken van gaten in bestaande procedures en protocollen. Daarnaast probeert de social engineer misbruik te maken van direct voor iedereen toegankelijke informatie, of informatie op een slimme manier te ontfutselen.
De meest voorkomende cybercrime-activiteit is het aanbod van illegale diensten en producten via internet, zoals internetcasino's of medische preparaten.
De overlast hiervan is het laatste jaar stabiel gebleven. De overlast door virussen, digitale spionage of computerinbraak is de afgelopen jaren zelfs afgenomen, waarschijnlijk door betere beveiliging. Voor de toekomst is de verwachting dat de meeste last zal worden veroorzaakt door het aanbod van illegale diensten en producten, en door computervirussen of -wormen. Vanuit beveiligingsoptiek is de grootste zorg het thuis inloggen op het bedrijfsnetwerk, draadloze netwerken en removable media (zoals USB flash drives en portables drives).

Inzet voorkomen en bestrijden cybercrime is groot

Overheidsinzet digitale criminaliteit niet onderschatten

'Overheid slecht voorbereid op cybercrime' kopten diverse media naar aanleiding van een recent verschenen rapport van een accountantskantoor. De noodklok wordt geluid, na een enquête onder respondenten uit bedrijfsleven en (semi)overheden. Met name de overheid zou te weinig aandacht hebben voor de gevolgen van criminaliteit met behulp van het internet. Het rapport doet geen recht aan de inspanningen die de overheid pleegt. Overigens sámen met de markt en internationale partners.

Aandacht voor de risico's van cybercrime is belangrijk, vindt ook GOVCERT.NL. Sterker nog, zij werkt al jaren aan het voorkomen van internetcriminaliteit en het oplossen van incidenten die daarmee te maken hebben. Daarnaast is de organisatie, met vele partners uit bedrijfsleven, de internationale security community en opsporingsdiensten, bezig met het bevorderen van het bewustzijn bij bedrijven, overheidsorganisaties en – niet te vergeten – de computergebruiker thuis. Op een praktische én effectieve manier, zonder angst te zaaien.

Steeds meer deelnemers

Al in 2002 werd GOVCERT.NL opgericht. Dit vanuit de vaste overtuiging dat het internet niet alleen zegeningen, maar ook risico's met zich mee zou brengen. Inmiddels zijn alle departementen en daarnaast nog vele andere – aan de overheid gelieerde– organisaties deelnemer van GOVCERT.NL. Er is vooral de laatste jaren een toename in het deelnemeraantal te zien, met name onder gemeenten. Al deze deelnemers zijn zich bijzonder bewust van de risico's van cybercrime, in welke vorm dan ook. De zonderlinge hacker die een overheidswebsite 'defaced', speciaal geschreven virussen of wormen, de inzet van botnets om sites plat te leggen: de rijksoverheid is zich wel degelijk bewust van alle gevaren die ICT-systemen lopen. Deelnemers worden op de hoogte gesteld van zwakke plekken, geïnformeerd over concrete dreigingen of over verhoogde dreigingsniveaus, over protocollen hoe om te gaan met persoonsgegevens en andere gerubriceerde informatie. We kennen allemaal immers de risico's van het verliezen of verkeerd gebruiken van gegevens die via mobiele datadragers worden overgebracht. Niet voor niets riep staatssecretaris Bijleveld van het ministerie van BZK bij de presentatie van de GOVCERT-publicatie 'Trendrapport 2007, Cybercrime in trends en cijfers' gemeenten op om deelname aan GOVCERT.NL te overwegen en waarschuwde zij voor de grote gevolgen van onvoldoende beveiliging van ICT-systemen.

GOVCERT.NL is het Computer Emergency Response Team (CERT) van de Nederlandse overheid. In andere woorden: de digitale brandweer van de overheid. De organisatie, opgericht in 2002 door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, draagt bij aan het voorkomen en afhandelen van ICT beveiligingsincidenten, 24 uur per dag, 7 dagen per week. Daarbij maakt zij gebruik van een breed (inter)nationaal netwerk. Zij ondersteunt organisaties die een publieke taak uitvoeren, zoals overheidsinstellingen, en werkt samen met vitale sectoren, zoals de bancaire sector, water- en energiebedrijven. Onderdeel van GOVCERT.NL is Waarschuwingsdienst.nl die computergebruikers thuis en in het kleinbedrijf (gratis) waarschuwt voor dreigende gevaren vanaf het internet. GOVCERT.NL is onderdeel van GBO.Overheid.

Ondersteuning bij incidenten

Het in het onderzoeksrapport gesignaleerde gebrek aan noodplannen voor het geval er zich ICT-gerelateerde incidenten voordoen, geldt wellicht voor andere sectoren, maar in mindere mate voor de overheid. Veel van de ICT-dienstverlening bij overheden is uitbesteed. Onderdeel van de afspraken die worden gemaakt met de dienstverleners, is dat risico's van uitval en slechte beschikbaarheid van diensten contractueel worden overgedragen aan de dienstverlener. Escalatie bij incidenten maakt daar vrijwel

zonder uitzondering deel van uit. Daarnaast is de expertise en ondersteuning bij incidenten door GOVCERT.NL beschikbaar voor alle onderdelen van de Nederlandse overheid. Eigenlijk hoeft de Nederlandse overheid maar één telefoonnummer te onthouden als er een ICT-beveiligingsincident plaatsvindt: het 24x7 bereikbare nummer van GOVCERT.NL.

Leerpunten

Met regelmaat wordt door overheidsorganisaties geoefend op respons bij ICT-incidenten: per organisatie, sectoraal en overheidsbreed. Zo is één van de oefeningen in 2007 breeduit in het nieuws geweest: oefening Shift Control (zie ook het artikel "Kabinet oefent crisis door ICT-uitval"in Nieuwsbrief Crisisbeheersing van juni 2007). Dergelijke oefeningen leveren waardevolle leerpunten op en dienen niet als eenmalig gezien te worden.
Diverse organisaties werken dagelijks aan het veilig maken en houden van de systemen van overheden. Van buitenaf lijkt het zelfs alsof dat er zoveel zijn, dat er versnippering optreedt. De kenner ziet echter een consistente en effectieve, gestroomlijnde samenwerking tussen organisaties met diverse focussen en opdrachten.
Het Team High Tech Crime van de KLPD heeft tientallen speciaal opgeleide rechercheurs in dienst en ook is er specialistische capaciteit binnen de politieregio's. Er is expertise opgebouwd binnen het Openbaar Ministerie, binnen de NCTb en daarnaast is er in Nederland een meldpunt Cybercrime.

Informatieknooppunt

Ook wordt via het Programma 'Nationale Infrastructuur ter bestrijding van Cybercrime' (NICC) door de overheid geïnvesteerd in het ontwikkelen en ondersteunen van experimenten die kennis over cybercrime opleveren en tegelijkertijd een concreet knelpunt oplossen. Het NICC stimuleert daarbij anderen om de witte vlekken in de nationale infrastructuur in te vullen. Een belangrijk resultaat is de realisatie van het Informatieknooppunt Cybercrime, waarbij in een vertrouwelijke setting uitwisseling plaatsvindt van operationele ICT-beveiligings-kennis tussen de vitale sectoren en de KLPD, AIVD en GOVCERT.NL.

Samenwerking

Essentieel daarbij is de samenwerking die plaatsvindt om internetcriminaliteit te voorkomen, op te sporen en in te perken. Samenwerking met ISP's (internet service providers) bijvoorbeeld. Eén van de activiteiten van GOV-CERT.NL is de uitvoering van het project Notice and Take Down. De Nederlandse banken hebben zich samen met het programma NICC verenigd als opdrachtgever van dit project, om ervoor te zorgen dat de schade die door phishingsites wordt aangericht, zo veel mogelijk wordt beperkt. Bij GOVCERT.NL zijn in 2007 67 phishingsites gemeld, waarvan meer dan de helft binnen een dag uit de lucht is gehaald. Hoe? Door de nauwe samenwerking met Nederlandse én internationale ISP's en met internationale CERT-organisaties. Een wereldwijd, dagelijks functionerend netwerk, waarbinnen informatie, incidenten en kennis worden uitgewisseld.

Risicomanagement

Is dit alles voldoende? Nee, uiteraard niet. Daar waar de technische inzet wellicht optimaal is om security te waarborgen, kunnen de interne werkafspraken, het risico-management of de mens achter de computer nog altijd falen. Want, zoveel is duidelijk: het grootste risico voor de beveiliging zit op de bureaustoel. Risico's zullen er altijd blijven. Al was het alleen maar omdat internetcriminaliteit zo lucratief is, dat de georganiseerde misdaad zal blijven investeren in het kraken van systemen, het plegen van identiteitsfraude, het opzetten van phishingsites, het verzamelen van botnets en het afpersen van webwinkels. Het blijft een wapenwedloop om de cybercriminaliteit terug te dringen. Net zoals het moeilijk blijft roofovervallen, paspoortfraude en inbraken terug te dringen. Ook hiervoor geldt niet dat het een kwestie van onwetendheid of des-interesse is, maar van samenwerking, kennis, alertheid, voorlichting, technologie, bewustwording en het delen van expertise. Beveiliging van systemen tegen incidenten is een blijvend punt van aandacht en vraagt voortdurend om investering door alle betrokken partijen.

Burgers, bedrijven en overheden

De zonderlinge hacker is inmiddels een dikbetaalde ingehuurde kracht van misdaadorganisaties. Internet én internetcriminaliteit kennen geen grenzen. Hoe goed de technologische mogelijkheden ook zijn, er blijven risico's en zwakke plekken. Echter, er is geen grond om aan te nemen dat burgers reden hebben om de aandacht en investering van de overheid in de beveiliging van systemen in twijfel te trekken. Wat wel belangrijk is, is dat diezelfde burger beseft dat internetgebruik risico's met zich meebrengt. Want juist het volledige vertrouwen in de beveiliging van je computer, maakt je het meest kwetsbaar. Dat geldt voor burgers, dat geldt voor overheden en voor het bedrijfsleven. Voor die taak van bewustwording staan wij gezamenlijk: als politiek, als industrie, als opsporings-diensten, als overheidsorganisaties en ook als accountants-bureaus.

Ella Broos, *woordvoerster,*
Douwe Leguit en Aart Jochem, *teamleiders GOVCERT.NL*

GOVCERT.NL

Oefening Civil Rhino: civiel-militaire samenwerking bij grootschalige evacuatie

In Nederland is een overstromingsramp een van de grote dreigingen. De omvang van de schade, het aantal getroffenen en slachtoffers zal groot zijn. Bij een grootschalige evacuatie zijn vele partijen betrokken. Rijk, provincies, gemeenten en veiligheidsregio's zijn verantwoordelijk voor het nemen van besluiten tijdens het evacuatieproces. Waterbeheerders voorzien de partijen van informatie over dreiging en ernst van de verwachte overstroming. Hulpdiensten, zoals politie, brandweer, GHOR en Rode Kruis, eventueel ondersteund door Defensie, laten de evacuatie soepel verlopen.

Bij militaire bijstand wordt doorgaans gedacht aan grote aantallen personen of specifiek materieel, zoals momenteel het mobiele hospitaalsysteem in Twente. Minder bekend is dat Defensie ook stafcapaciteit biedt ter ondersteuning van civiele crisisbesluitvorming. Militaire (onder)officieren kunnen worden ingezet als aanvullende capaciteit op een civiele crisisstaf in bijvoorbeeld een 'landelijk operationeel team'. Zelfs inzet voor een veiligheidsregio is niet ondenkbaar. Op verzoek van de civiele autoriteit kunnen de militairen onder zijn of haar gezag en leiding alle taken en processen uitvoeren waarvoor niet voldoende civiele crisismanagementcapaciteit beschikbaar is. Analytisch denken, situaties in kaart brengen, werken volgens scenario's en onder grote tijdsdruk, zijn vaardigheden waarover militairen immers ook voor hun reguliere staftaken moeten beschikken. Wel moeten de militaire (onder)officieren eerst leren optreden in civiele samenwerkingsverbanden en wennen aan andersoortige crises: een industriële calamiteit of een natuurramp in eigen land in plaats van een gewapend conflict of een vredesoperatie in Afghanistan. En de civiele partijen moeten wennen aan (de idee aan) militairen in hun organisaties.

Verschillende zulu's

De grootte van de stafcapaciteit kan variëren van enkele personen tot aan een staf van zo'n 50 militairen om "klokrond" op te treden. De stafcapaciteit kan voorzien in eigen communicatiemiddelen en uitgerust worden met procesondersteunende middelen zoals het *Integrated Staf Information System* (ISIS). Hiermee kan de actuele operationele situatie in kaart worden gebracht. Aangezien de civiele rampenbestrijding en de krijgsmacht beide een eigen werkwijze, mogelijkheden, beperkingen en cultuur hebben, is multidisciplinair oefenen een vereiste. Beide werelden moeten elkaar goed begrijpen en elkaars taal leren spreken om adequaat te kunnen samenwerken.

Samen met civiele instanties in Brabant heeft majoor Erik Backus, hoofd Bureau Nationale Operaties bij het Regionaal Militair Commando Zuid, een praktijkgericht kennismakings- en trainingsprogramma opgezet om een brigadestaf en de civiele partners aan elkaar te laten wennen en te leren samenwerken. Backus: "We zijn begonnen met de staf van de 13e Gemechaniseerde brigade uit Oirschot. Onlangs teruggekeerd van de vredesoperatie in Afghanistan focust deze eenheid zich dit jaar op het thema 'nationale operaties'. In een tweedaags seminar voor de staf hebben de rampenbestrijdingsdiensten, een waterschap, een gemeenteambtenaar en het NIFV uitleg gegeven over de organisatie van rampenbestrijding en crisisbeheersing in

Nederland. Een eerste noodzakelijke stap om elkaars mogelijkheden te leren kennen en dezelfde taal te leren spreken. Elke organisatie heeft zijn eigen jargon. Als een politiefunctionaris bijvoorbeeld vraagt om een 'zulu', bedoelt hij helikopterondersteuning, terwijl een militair met diezelfde 'zulu' een ziekenwagen bedoelt".

Continu up to date

Om de praktijk te trainen vond Backus in 's Hertogenbosch onder het provinciehuis van Noord-Brabant de commandobunker. "Ik wilde de mensen van het kazerneterrein af hebben om het opzetten van een staf in een civiele omgeving te leren oefenen", aldus Backus. De provincie stelde voor om óók voor de eigen organisatie en voor de andere civiele partners oefendoelen aan de oefening te verbinden en een gezamenlijke crisisstaf te formeren die een groot scenario moest afhandelen".

Waar het op aankomt, is 'scenario denken' en intellectuele capaciteit

Uiteindelijk werd een plan geboren voor een driedaagse stafoefening van 15 tot en met 17 januari, waarbij een bovenregionale planningsstaf een grootschalige evacuatieoperatie wegens een dreigende overstroming voor de kiezen kreeg. "Zo'n scenario leent zich bij uitstek voor militaire stafondersteuning, omdat een evacuatieplan arbeidsintensief is en veel stafcapaciteit vraagt", vervolgt Backus. "In deze oefening hebben we onze eigen staffuncties '*current*' en '*plans*' samengebracht in een gezamenlijke stafstructuur met brandweer, politie, Rode Kruis, provincie, waterschappen en Omroep Brabant in de functie van rampenzender. '*Current*' is het deel van de staf dat continu zorgt voor een *up to date* operationeel beeld van de calamiteit, zodat iedereen op ieder moment over de meest actuele informatie beschikt. De sectie '*plans*' maakt de daadwerkelijke planning voor de uit te voeren acties".

Vermogen om vooruit te plannen

De Brabantse commissaris van de Koningin Hanja Maij-Weggen woonde delen van de oefening bij. "Wat ik zag, was een samenwerking en samenspel die aanvankelijk wat aarzelend waren. Maar het is opvallend hoe snel die aarzeling verdween. In zeer korte tijd is er geconcentreerd en met inzet gewerkt. Het verschil tussen de mensen in het groen, het blauw, de gemeenten en de provincie verdween. Er ontstond een team. Dat geeft vertrouwen." De meerwaarde van deze vorm van samenwerking met Defensie is voor de commissaris geen vraag. "Vooral het vermogen om vooruit te plannen is een goede aanwinst. Ik denk ook dat de inzet van militaire middelen bij de

bestrijding van rampen hierdoor beter gecoördineerd wordt. Het was een positieve ervaring voor alle veiligheidspartners".

Anton Aerts, werkzaam bij het bureau Conflict en Crisisbeheersing (CCB) van de politie Brabant Zuid-Oost beaamt dat. Van nabij zien hoe militairen op stafniveau problemen aanpakken was voor hem een nieuwe ervaring. "De structuur die ze gebruiken, vind ik heel bijzonder, met een splitsing tussen de afdeling *current* en *plans*. Mooi was om te zien dat men deze structuur ook wist om te buigen naar het adviseren van het civiel gezag en zo – al werkend – op één lijn kwam. Daarbij was opvallend veel openheid en ruimte om dingen uit te proberen en ideeën aan te dragen. Ook voor mijzelf om de kennis vanuit mijn werkveld in te brengen," aldus Aerts.

Majoor Backus ziet dat leereffect ook voor de militaire staf. "Doel van de oefening was om het 'civiele bewustzijn' bij onze mensen te versterken. Nu moeten we de procedures en werkwijzen meer op elkaar afstemmen en dat kan alleen door intensieve kennismaking en gezamenlijk oefenen. Wij hopen dat we in de gelegenheid worden gesteld om veel met civiele partners in de veiligheidsregio's te oefenen, ook met de andere brigadestaven".

Arnoud Reijnen, coördinator woordvoering en crisiscommunicatie van de provincie Noord-Brabant, prijst het oefenen aan als een 'geweldige leerervaring'. "Duidelijk komt tot uiting dat militairen een enorme routine hebben in oefenen en in het omgaan met dynamische crisissituaties. Dat zijn eigenschappen waar alle civiele partners in daadwerkelijke grootschalige crisissituaties echt van kunnen profiteren".

J.M. Schalk,
wnd. hoofd Bureau Communicatie en Externe Betrekkingen, Regionaal Militair Commando Zuid

Met dank aan: Rob Jastrzebski (Vakblad Incident)

De Staat van het Klimaat 2007

"Klimaatverandering biedt kansen voor innovatie, zowel bij de vermindering van de uitstoot van broeikasgassen als bij het anticiperen op de gevolgen." Dat stellen Nederlandse klimaatwetenschappers in de brochure 'De Staat van het Klimaat 2007'.

Deze jaarlijkse inventarisatie van de stand van zaken en nieuwe ontwikkelingen op het gebied van klimaatonderzoek en klimaatbeleid is op 19 februari aangeboden aan minister president Jan Peter Balkenende. *De Staat van het Klimaat 2007* is samengesteld door het Platform Communication on Climate Change (PCCC) waarin vooraanstaande Nederlandse kennisinstituten op het gebied van klimaat samenwerken. Een greep uit de onderwerpen: wat hebben we concreet in 2007 gemerkt van de klimaatverandering, de betekenis van het vorig jaar verschenen IPCC-klimaatrapport van de Verenigde Naties met ook een vertaling naar de Nederlandse situatie, nationaal en Europees beleid, waar mogelijk vergaande besluiten over zijn genomen, nieuwe technieken om CO_2-uitstoot te verminderen en onderzoek naar het klimaatbestendig maken van Nederland. Met de toename van het wetenschappelijk onderzoek groeit ook de kennis van het klimaatsysteem, die wordt ingezet bij de ontwikkeling van klimaatbeleid. De auteurs van de brochure signaleren positieve beleidsontwikkelingen op nationaal, Europees en mondiaal niveau. Om de klimaatverandering te temperen, wordt in Europa ingezet op meer energiebesparing, een groter aandeel hernieuwbare energie en versterking van het emissiehandelssysteem. Maar ook als we erin slagen om de uitstoot van broeikasgassen sterk te verminderen, verandert het klimaat. Natuurlijke en maatschappelijke sectoren moeten zich instellen hiermee om te gaan.
In deze nieuwste Staat van het Klimaat worden nieuwe ontwikkelingen gesignaleerd rond waterbeheer, omgaan met een groter overstromingsrisico en klimaatbestendiger natuur.

Voor meer informatie: **www.klimaatportaal.nl**
De brochure is te bestellen via ottelien.vansteenis@wur.nl.

VS en Nederland samen in crisisbeheersing

Het COT Instituut voor Veiligheids- en Crisismanagement gaat met enkele gerenommeerde Amerikaanse instituten samenwerken op het gebied van crisisbeheersing. Staatssecretaris Tineke Huizinga van Verkeer en Waterstaat ondersteunt dit initiatief de komende drie jaar met een bijdrage van 1 miljoen euro.
Huizinga en COT-voorzitter Uri Rosenthal ondertekenden op 7 maart in New Orleans de bijbehorende overeenkomst. Aan Amerikaanse zijde gaat het om de universiteiten van Colorado en Delaware en de George Washington University in Washington, die hun kennis over het omgaan met natuurrampen inzetten. Bij laatstgenoemde universiteit zal het secretariaat van het Nederlands-Amerikaanse consortium worden gevestigd. Een van de initiatiefnemers is Eelco Dykstra, 'rampenhoogleraar' aan de George Washington University en voormalig Amerika-correspondent van de *Nieuwsbrief Crisisbeheersing*. Hij schreef een paar maanden na de verwoestende orkaan Katrina een boekje over een vergelijkbare fictieve natuurramp in Nederland. Volgens Dykstra heeft Nederland veel kennis in huis over preventie, zoals het voorkomen van overstromingen.
De Amerikanen blinken uit in operationele ervaring, bijvoorbeeld door het in kaart brengen van ervaringen van het grote publiek en hulpdiensten. In november wordt in Nederland gedurende een hele week onder de naam 'Waterproef' geoefend met overstromingsrampen.

Voorbereiding op rampen verbetert, maar tempo moet omhoog

Dat schrijft minister Ter Horst op 12 maart aan de Tweede Kamer naar aanleiding van een rapport van de Inspectie OOV over de periode 2003-2007 en op basis van rapportages van Commissarissen van de Koningin.
De Inspectie OOV constateert dat het basisniveau van de voorbereiding op rampen is gestegen. Tekortkomingen zijn er nog bij de voorbereiding op drie belangrijke processen die de startmotor van de rampenbestrijding zijn: informatiemanagement, leiding en coördinatie en opschaling.
Minister Ter Horst wil de kwaliteitsverbetering doorzetten en versnellen via het wetsvoorstel op de veiligheidsregio's en bijbehorende kwaliteitseisen, via afspraken in het bestuursakkoord met de gemeenten en via convenanten met de regio's. Als een regio een convenant met de minister afsluit, is er ook extra geld beschikbaar (1,3 tot 1,8 miljoen euro per regio).

De provincies constateren dat de hulpverleningsdiensten in de regio's een grote ramp niet aan kunnen. Minister Ter Horst schrijft dat in zo'n geval bijstand van andere regio's voor extra capaciteit moet zorgen. Het Landelijk Operationeel Coördinatie Centrum (LOCC) ondersteunt de regio's bij het beter organiseren van bijstand. Ter Horst wil het risicobewustzijn bij lokale en regionale bestuurders vergroten. Het zijn namelijk de bestuurders in de regio's die de capaciteit van de hulpverlening moeten vaststellen. Zij moeten de capaciteit afzetten tegen de risico's, de zelfredzaamheid van inwoners en de mogelijkheden voor bijstand uit andere regio's. Als de Wet op de veiligheidsregio's van kracht wordt (vermoedelijk vanaf 2009), moeten de regio's minimaal voldoen aan de basisvereisten crisismanagement.

Dreigingsniveau in Nederland verhoogd naar substantieel

Hoewel er geen concrete aanwijzingen voor aanslagen in Nederland zijn, geeft de toegenomen internationale terroristische dreiging aanleiding tot het verhogen van het algemene dreigingsniveau voor Nederland van beperkt naar substantieel. Dit concludeert de Nationaal Coördinator Terrorismebestrijding in zijn nieuwe Dreigingsbeeld Terrorisme Nederland (DTN), waarvan de samenvatting op 6 maart door de ministers Hirsch Ballin (Justitie) en Ter Horst (Binnenlandse Zaken en Koninkrijksrelaties) naar de Tweede Kamer is gestuurd. Met de verhoging van de dreiging is het dreigingsniveau op het niveau zoals dit gold sinds de start van het DTN in mei 2005 tot april 2007. In de tussenliggende periode was de dreiging beperkt.

Sinds de zomer van 2007 is sprake van een toename van de internationale invloed op de jihadistische dreiging in West-Europa. Bij aanhoudingen in het Verenigd Koninkrijk (juni 2007), Denemarken (september 2007) en Duitsland (september 2007) bleek sprake van training en soms van strategische sturing door aan al Qa'ida gelieerde groeperingen in onder meer Pakistan en Afghanistan. In de beoordeling van de invloed uit Pakistan en Afghanistan moet worden meegenomen dat daar al geruime tijd een zeker herstel van de kern van al Qa'ida gaande is. Uit een recente Spaanse casus (januari 2008) blijkt dat de aanslagplegers niet eerder in Europa waren, maar lijken te zijn ingevlogen vanuit het grensgebied Pakistan/Afghanistan. Het handelt zich bij dergelijke jihadisten om een groep die beter en meer praktijkgericht is getraind dan de meeste in Europa woonachtige jihadisten. Kennis opgedaan uit recent verijdelde aanslagen in Europa maakt het voorstelbaar dat in West-Europa, en dus ook Nederland, meer dan voorheen rekening moet worden gehouden met een aanslag. De dreiging gaat hoofdzakelijk uit van aan de kern van al Qa'ida gerelateerde groepen uit Pakistan en Afghanistan. Daar komt bij dat Nederland de afgelopen tijd negatief in beeld is gekomen in de islamitische wereld door de wijze waarop discussie over de islam in Nederland door sommigen wordt gevoerd, bijvoorbeeld naar aanleiding van een aangekondigde film over de Koran. Positief is dat in het huidige DTN wederom gesignaleerd wordt dat Nederlandse moslims zich opmerkelijk weerbaar opstellen tegen radicalisering en extremisme. De beschreven internationale invloed op de dreiging geeft aan dat de zichtbaarheid daarvan voor Europa afneemt: radicalisering, netwerkvorming en training vinden in het buitenland plaats en dus veelal buiten het zelfstandige zicht van de Europese inlichtingen- en veiligheidsdiensten. Desalniettemin zijn dankzij internationale samenwerking in Nederland in de afgelopen periode ook nieuwe personen onderkend via wie mogelijk een internationale dreiging kan uitgaan tegen Nederland of andere Europese landen.

(bron: persbericht NCTb)

Mijn Mening

In de rubriek "Mijn Mening" reageren lezers op een artikel in dit Magazine. Een reactie van maximaal 450 woorden moet inhoudelijk interessant zijn. Bijdragen zijn welkom op het e-mailadres **crisisbeheersing@minbzk.nl** onder vermelding van "Mijn Mening" en naam en adres afzender. De redactiecommissie behoudt zich het recht voor om een reactie zonder overleg te weigeren of in te korten.

Burgerparticipatie en zelfredzaamheid: *What's in it for* burgers?

Hierbij reageer ik op de artikelen over zelfredzaamheid en burgerparticipatie bij rampen en crises in het januarinummer. Kern van alle artikelen is hoe belangrijk professionele groepen burgerparticipatie en zelfredzaamheid in de rampenbestrijding en crisisbeheersing vinden. De vraag in hoeverre burgers het belangrijk vinden dat zij actief worden voor hun eigen en andermans veiligheid komt helaas niet aan bod. Terwijl dit een noodzakelijke voorwaarde is voor een succesvolle burgerparticipatie en zelfredzaamheid op het terrein van de nationale veiligheid.

Het is niet mijn bedoeling om in deze reactie de waarde van burgerparticipatie en zelfredzaamheid in twijfel te trekken. Wel wil ik een vijftal kantekeningen plaatsen bij de artikelen over dit onderwerp.
Mijn eerste opmerking gaat over de veranderende houding van professionele groepen jegens burgers. Immers in de loop van de tijd hebben professionele groepen steeds meer burgers van zich afhankelijk gemaakt. Met als gevolg dat veel burgers passief zijn geworden als het gaat om de eigen veiligheid en die van anderen.
Ten tweede: door de overgang van de zogenaamde nachtwakersstaat (beperkte rol van de overheid) naar de verzorgingsstaat (dominante rol van de overheid en professionele groepen) hebben burgers een aanmerkelijk deel van hun inkomen overgedragen aan de overheid. Veelal met de bedoeling en de verwachting dat de overheid met haar professionele groepen namens de burgers publieke taken zoals veiligheid voor de burgers uitvoert.
Ten derde: na deze overdracht van financiële middelen en taken ligt de bereidheid van burgers om actief te participeren of zelfredzaam te worden niet direct voor de hand Daarnaast is er in toenemende mate druk op geld en tijd. Hierdoor zijn burgers steeds minder in staat en bereid om zelf actief te zijn op het gebied van de nationale veiligheid.
Ten vierde: uit Amerikaans onderzoek blijkt dat burgers pas actief willen worden indien burgers veel vertrouwen in het overheidsoptreden hebben. Eerst moet de overheid z'n eigen zaakjes goed op orde hebben en dan pas is er een grotere kans op actief burgerschap in de veiligheid. Zodra burgers verwachten dat zij onvolkomenheden van de overheid moeten compenseren, zal de bereidheid van burgers niet zo groot zijn. Terwijl de behoefte aan hulp juist groot is.
Mijn vijfde en laatste opmerking is dat burgers eerder duurzaam zullen willen bijdragen aan de preparatie- en responsfase van een ramp of crisis, als er niet alleen voordelen voor de overheid zijn, maar ook voor burgers. Dit betekent dat er voor burgers niet alleen maar lasten moeten zijn, maar ook incentives.
Mijn conclusie is dan ook: zolang enkel en alleen de belangen van de overheid en professionele groepen worden gediend, zal van een duurzame burgerparticipatie en zelfredzaamheid geen sprake zijn.

dr. Gerrit Haverkamp,
directie Strategie, afdeling voor Internationale Samenwerking, ministerie van BZK

[1] *Aangehaald in: G. Haverkamp, Vuur als gemeenschappelijke vijand, Den Haag 2005, pp. 154-155.*

Conferentie "Risk meets Crisis" 21-22 mei 2008

Op 21 en 22 mei a.s. wordt het internationale congres "Risk meets Crisis" georganiseerd in het Carlton Beach Hotel in Scheveningen. Het congres is de slotbijeenkomst van twee Europese projecten in het kader van Interreg North Sea Region, namelijk Safecoast en Chain of Safety. Beide projecten hebben zich beziggehouden met kustoverstromingen, ieder vanuit hun eigen invalshoek. Het project Safecoast heeft zowel een technische als strategische benadering gekozen om te komen tot gemeenschappelijke oplossingen voor de risico's van kustoverstromingen en erosie langs de Noordzeekust, terwijl het project Chain of Safety zich richt op wederzijdse samenwerking, kennisuitwisseling en hulpverlening tussen de Noordzeelanden wanneer zich onverhoopt een kustoverstroming zou voordoen.
Safecoast heeft alles te maken met risicomanagement (hoe houden we het water tegen?) en Chain of Safety met crisismanagement (hoe beperken we de gevolgen zoveel mogelijk, wanneer het eerstgenoemde niet lukt?).

Voor meer informatie over de projecten en/of het congres:
www.safecoast.org
www.chainofsafety.com

CHAIN OF SAFETY
covering the whole north sea region

Colofon

Redactieadres
Postbus 20011, 2500 EA Den Haag
E-mail: crisisbeheersing@minbzk.nl
Internet: **www.minbzk.nl/veiligheid**

Redactiecommissie
Redactiecommissie: Henk Geveke, Nico de Gouw en Geert Wismans (samenstelling en eindredactie)
Redactiemedewerker: Maddy Ockhorst (070-426 7011)
Redactiesecretariaat: Nalini Bihari (070-426 73 54)

Redactieraad
Prof. dr. Ben Ale (Technische Universiteit Delft)
Prof. dr. Joost Bierens (VU Medisch Centrum Amsterdam)
Dr. Arjen Boin (Louisiana State University, USA)
Mr. dr. Ernst Brainich von Brainich Felth
Dr. Menno van Duin (Nederlands Instituut Fysieke Veiligheid)
Prof. dr. Georg Frerks (Universiteit Wageningen)
Prof. dr. Bob de Graaff (Universiteit Leiden/Campus Den Haag)
Prof. dr. Ira Helsloot (Vrije Universiteit Amsterdam)
Prof. dr. Erwin Muller (Universiteit Leiden)
Prof. dr. Uri Rosenthal (Universiteit Leiden)
Dr. Astrid Scholtens (Politieacademie/Nederlands Instituut Fysieke Veiligheid)
Prof. dr. Erwin Seydel (Universiteit Twente)
Prof. dr. Rob de Wijk (The Hague Centre for Strategic Studies)

Aan dit nummer werkten mee:
Eva Barneveld, Guido Bertolaso, Linda Bontje, Anja van den Bosch-Overduin, Bart Boon, Ella Broos, Ruth Clabbers, Simon van der Doorn, Matthew Elkington, Natasja Hartzema, Gerrit Haverkamp, Ira Helsloot, Mw. G. ter Horst, Jasper van der Horst, Aart Jochem, Ian Kearns, Erik Klaver, Patrick Lagadec, Roos Lamers, Douwe Leguit, Bruce Mann, Ron de Meijer, Eimert van Middelkoop, Monique Otten, Katie Paintin, Eric Pruyt, Sebastian Reyn, José Schalk, Dick Schoof, Michael Thornton, Frank Vergeer, Michiel Verlaan, Jacob Verschuur, Bert Visser, Peter de Wit

Fotografie
Croptrust, Defensievoorlichting, Arenda Oomen, Rob Jastrzebski, Shell

Vormgeving
Grafisch Buro van Erkelens, Den Haag

Productiebegeleiding
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Communicatie en Informatie / Grafische en Multimediale Diensten

Druk
OBT bv, Den Haag

ISSN 1875-7561

Voor een gratis abonnement mail: crisisbeheersing@minbzk.nl.
Het magazine is te downloaden via www.minbzk.nl/veiligheid.

Vier vragen aan:

Eimert van Middelkoop, minister van Defensie naar aanleiding van aftrap Verkenningen op 5 maart

Waarom worden er verkenningen uit gevoerd?

"Het kabinet kiest voor een actieve en constructieve rol van Nederland in de wereld. Hierbij hoort een moderne en professionele krijgsmacht die overal maatwerk levert.
De defensiebegroting is voor deze kabinetsperiode sluitend. Niettemin is er reden te bezien hoe het financiële beeld er in de toekomst uitziet. Dit is nodig voor een stabiele ontwikkeling van de krijgsmacht. Ook moeten militairen en burgers die in opdracht van onze samenleving risico's lopen het perspectief behouden op een toekomstbestendige krijgsmacht. Met de verkenningen willen wij een inhoudsvolle bijdrage leveren aan de oordeelsvorming over de krijgsmacht en het daarmee samenhangende niveau van defensiebestedingen. Om de taken en de middelen van de krijgsmacht ook op de langere termijn in evenwicht te houden hebben wij besloten verkenningen uit te voeren."

Wat is het doel van de verkenningen?

"Voor deze kabinetsperiode bieden de uitgangspunten van de beleidsbrief "Wereldwijd dienstbaar" voldoende houvast voor een "toereikende krijgsmacht". Het huidige ambitieniveau past naadloos bij de actieve en constructieve rol die het kabinet in de wereld wil spelen. Dat wij nu aan verkenningen naar de toekomst van de krijgsmacht beginnen, moet daarom eerst en vooral worden uitgelegd als een uitdrukking van onze politieke wil ook voor de toekomst recht te doen aan de vereisten van dat centrale instrument van onze staat.
Het wordt tijd dat Nederlanders beginnen te wennen aan het idee dat behalve lágere, ook hógere defensie-uitgaven denkbaar zijn. Dat deze zelfs nodig kúnnen zijn, wil ons land zich veilig wanen en een actieve bijdrage blijven leveren aan de internationale vrede en veiligheid. Tevens koester ik de voorzichtige hoop dat deze kabinetsperiode voor de krijgsmacht in dat opzicht als een historisch omslagpunt zal worden beschouwd. Bij een welvarend land als Nederland, met zijn grote economische belangen en krachtige morele drijfveren, hoort een moderne, robuuste en geloofwaardige krijgsmacht.
De verkenningen leggen de basis voor een krijgsmacht die blijvend tegen de toekomst is bestand. De verkenners hebben de volgende opdracht mee gekregen: de verkenningen dienen, op grond van de op langere termijn te verwachten ontwikkelingen en mogelijke scenario's, zonder beperkingen beleidsopties te formuleren met betrekking tot de toekomstige ambities voor de Nederlandse defensie-inspanning, de daaruit voortvloeiende samenstelling en toerusting van de krijgsmacht en het daarbij behorende niveau van de defensiebestedingen. Defensie heeft alle reden om deze verkenningen vol zelfvertrouwen in te gaan. De verkenningen zullen de basis leggen voor een krijgsmacht die blijvend tegen de toekomst is bestand. De grillige wereld waarin wij leven staat niet toe dat wij nonchalant met de vereisten van onze krijgsmacht omgaan. Het motto voor de verkenningen luidt ook niet voor niets: *Houvast voor de krijgsmacht van 2020.*"

Hoe worden de verkenningen opgepakt en uitvoerd?

"De verkenningen worden opgepakt en uitgevoerd door een interdepartementale projectdirectie met deelname van de ministeries van Defensie, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Financiën en Justitie. Daarnaast is er duidelijke externe betrokkenheid. Een klankbordgroep van zeven deskundigen, onder voorzitterschap van oud-minister Gerrit Zalm, zal de verkenningen kritisch volgen en daarover gevraagd en ongevraagd advies uitbrengen.
De verkenningen zijn gediend van een zo analytisch mogelijk aanpak. Ze worden uitgevoerd aan de hand van twee invalshoeken. Enerzijds gaat het om ontwikkelingen die van invloed zijn op de omvang en de aard van het beroep dat in de toekomst op de krijgsmacht wordt gedaan (de 'vraagzijde'). Hierbij zijn de veranderende internationale verhoudingen en de veiligheidssituatie binnen en buiten onze landsgrenzen belangrijke aandachtsgebieden. Ook de maatschappelijke rol van de krijgsmacht wordt bezien. Anderzijds wordt gekeken naar ontwikkelingen die van invloed zijn op de krijgsmacht als organisatie (de 'aanbodzijde'). Zo hebben de veranderende inzet van de krijgsmacht en operationele ontwikkelingen onmiskenbaar organisatorische gevolgen."

Wat is het belang van de verkenningen voor nationale veiligheid en crisisbeheersing?

"Eén van de hoofdtaken van Defensie is het ondersteunen van de civiele autoriteiten bij nationale veiligheid en crisisbeheersing. Hiertoe zijn onder meer afspraken gemaakt over structurele vormen van civiel-militaire samenwerking. De verkenningen zullen inzicht moeten geven welke defensie-inspanningen nodig zijn om ook in de toekomst de nationale veiligheid mede te kunnen waarborgen."