Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

jaargang 10 | nummer 1 | **februari 2012**

Magazine

nationale veiligheid en crisisbeheersing

Thema: Publiek private samenwerking
Cyber Security Strategie stevig in de steigers
Bestrijding hoogwater: alertheid en rationele communicatie

Inhoud

THEMA: PUBLIEK PRIVATE SAMENWERKING

OVERIGE ONDERWERPEN

Het Magazine nationale veiligheid en crisisbeheersing is een tweemaandelijkse uitgave van de Nationaal Coördinator Terrorisme-bestrijding en Veiligheid van het ministerie van Veiligheid en Justitie.
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.

Omslagfoto:
Eric Sijtsma

Oefenen met burgers en bedrijven noodzakelijk

Ik zal het maar bekennen, ik ben een groot voorstander van publiek private samenwerking. Niet alleen op het terrein van de criminaliteitsbestrijding en de beveiliging maar ook op het brede gebied van de crisisbeheersing en rampenbestrijding. Bij criminaliteitsbestrijding en beveiliging is het inmiddels toch redelijk gewoon dat burgers, bedrijven en overheid elkaar weten te vinden. Natuurlijk ken ik de studies die ook de problemen die daarbij zich voordoen beschrijven. Maar dominant in dat veld is dat de overheid niet alleen in staat is om de criminaliteit te bestrijden of winkelgebieden of bedrijventerreinen te beveiligen. Daar heeft al veel langer de overtuiging post gevat dat burgers en bedrijven een rol moeten spelen. Dat gebeurt dan ook, niet alleen incidenteel en in projecten maar ook structureel.

prof. mr. dr. E.R. (Erwin) Muller,
hoogleraar Veiligheid en Recht
Universiteit Leiden
wetenschappelijk directeur Instituut
voor Strafrecht en Criminologie
Universiteit Leiden

Binnen de rampenbestrijding en crisisbeheersing is de rol van burgers en bedrijven veel minder normaal en geaccepteerd. We spreken al lang over eigen verantwoordelijkheid en zelfredzaamheid van burgers. Het blijft echter bijzonder moeilijk om daar daadwerkelijk invulling aan te geven. De rol van bedrijven en publieke organisaties (niet zijnde hulpverleningsdiensten) bij crisisbeheersing en rampenbestrijding is helemaal nog nauwelijks vormgegeven. Het lijkt er eigenlijk op dat de overheid bij de rampenbestrijding en crisisbeheersing er van uit gaat dat zij dit alleen kan en dat enige vorm van hulp vanuit de burgers of het bedrijfsleven eigenlijk niet nodig is. Ik denk dat dit een misvatting is. Burgers, bedrijven en publieke organisaties kunnen zeker helpen bij rampenbestrijding en crisisbeheersing.

Deze hulp kan uit vele aspecten bestaan. Het kan gaan om het snel informeren van de overheid over specifieke dreigingen of crises. De moderne en sociale media kunnen daarbij een belangrijke rol spelen. Bedrijven kunnen met behulp van hun kennis, middelen en machines mogelijk van dienst zijn bij specifieke rampen of crises. De overheid hoeft niet alles in eigen huis te hebben. Van risicovolle bedrijven kan – meer dan nu het geval is – gevraagd worden zich langere tijd tijdens een crisis zelf te kunnen redden. Burgers in de buurt van risicovolle industrie of in gebieden die mogelijk kunnen overstromen kunnen bijdragen aan de verbetering van de voorbereiding van wijken op eventuele rampen en crises door bijvoorbeeld zich te organiseren in buurten om echt klaar te zijn voor specifieke rampen. De overheid kan hieraan bijdragen. Niet alleen door voorlichtingscampagnes vorm te geven maar door ze daadwerkelijk de middelen en de voorzieningen te geven zodat zij zich kunnen voorbereiden.

Om dit allemaal te kunnen bereiken is het noodzakelijk om burgers en bedrijven veel meer dan nu het geval is actief te informeren over de dreigingen die specifiek voor hen van belang zijn. Dan gaat het niet om algemene dreigingen maar dreigingen die relevant zijn voor mevrouw X in straat Y of bedrijf Z in straat A. Het lijkt mij daarnaast heel goed als nu echt eens werk gemaakt gaat worden van rampenoefeningen met burgers en bedrijven. In Nederland oefenen we toch vooral met bestuurders, ambtenaren en hulpverleningsdiensten. Slechts heel zelden vindt een oefening plaats waarbij burgers en bedrijven een grote rol hebben. Pas als we in Nederland in staat en bereid zijn dat te doen kan van een volwaardige publiek private samenwerking op het terrein van de crisisbeheersing en rampenbestrijding sprake zijn.

Sinds 2006 wordt op Schiphol de beveiliging op een geïntegreerde en gestructureerde wijze gezamenlijk aangepakt door overheidspartijen en de luchtvaartsector. In het Platform Beveiliging en Publieke Veiligheid Schiphol (BPVS) worden op een effectieve en efficiënte manier de beveiligingsrisico's vertaald. Het publiek privaat samenwerkingsverband is een succes en boekt concrete resultaten in zowel het beheersen van beveiligings- en veiligheidsrisico's als het ondersteunen van de taken en processen van de respectieve partijen. Speerpunten van de samenwerking zijn onder meer het cameraproject, de integratie van grens- en securityprocessen, de veiligheids- en controlemaatregelen met betrekking tot het passagiers- en vrachtproces, de toegangscontrole en de communicatie.

Ruud Oord,
programmamanager, Beveiliging en Publieke Veiligheid Schiphol
Mirjam Snoerwang,
communicatieadviseur Schiphol

Publiek private samenwerking op Schiphol

Aanleiding voor geïntegreerde aanpak

De directe aanleiding voor de oprichting van BPVS was de zogenoemde 'diamantroof' die op 25 februari 2005 op Schiphol plaatsvond. Op het platform werd een overval gepleegd op een waardetransport. Nadat een partij diamanten uit de buik van het vliegtuig was overgeladen werd de chauffeur van de geldauto bedreigd.
De daders gingen er vandoor met de auto en een pakket diamanten met een waarde van 80 miljoen euro. Dit incident was groot en de aanleiding om een aantal andere incidenten op Schiphol onder de loep te nemen op het gebied van criminaliteit, illegale immigratie en smokkel. Als directe reactie hierop werd de Overheidscommissie Toegangsbeheer geformeerd. De aanbevelingen van deze commissie (later Commissie Oord) richtten zich op een geïntegreerde aanpak van de beveiligings- en veiligheidsrisico's met inachtneming van uitvoerbaarheid, de kosten en de effectiviteit.

Concreet werd voorgesteld:
- een centraal besturingsmodel in te richten. Voor regie en afstemming, gezamenlijke risico analyse, financiering en communicatie;
- een centraal gezamenlijk camerasysteem op te zetten om bestaande en nieuwe technologieën toe te passen om de processen te ondersteunen;
- de grens- en securityprocessen te integreren en zo een efficiencyslag te bereiken in het signaleren van risicopersonen, toepassing biometrische kenmerken en ID documenten;
- het structureel beheersen van alle in- en uitgangen door (onvoorspelbare) controles op passagiers en medewerkers.

Deze voorstellen voor een geïntegreerde aanpak kregen brede steun van de Tweede Kamer, Hierop is als gezamenlijke overlegstructuur op 25 januari 2006 het Platform Beveiliging en Publieke Veiligheid Schiphol (BPVS) opgericht.

Jos Nijhuis, Chief Executive Officer Schiphol:

'Bij een organisatie als Schiphol, waar zoveel partijen samenwerken en van elkaar afhankelijk zijn, moeten alle schakels goed in elkaar grijpen. Er mogen geen gaten vallen, maar er mag ook geen onnodig dubbel werk gebeuren. Daarvoor is centrale regie nodig. Efficiënte beveiligingsmaatregelen zijn essentieel voor een hub als Schiphol. De voorgeschreven beveiligingsmaatregelen zijn de afgelopen tien jaar fors in omvang toegenomen. Jaarlijks is daarmee een bedrag gemoeid van 250 miljoen euro, zo'n 40 procent van de exploitatiekosten. Al onze aandacht gaat uit naar de continuïteit van onze bedrijfsvoering en onze internationale concurrentiepositie. Daarbij zoeken we voortdurend naar de optimale balans tussen risicobeheersing en kosteneffectiviteit. De wettelijke regels vormen vanzelfsprekend ons kader. Hier geldt: 'no comply = no fly'. Maar tegelijkertijd wil je ook zo aantrekkelijk mogelijk zijn voor passagiers.'

Vliegende start met commitment op hoogste niveau

In het Platform zitten vertegenwoordigers van betrokken publieke en private partijen op beleidsniveau: ministeries van Justitie/NCTV, BZK, I&M, IVW, IND, gemeente Haarlemmermeer, Politie Kennemerland, Douane, Koninklijke Marechaussee. Aan de private kant vertegenwoordigers van Schiphol Group, luchtvaartmaatschappijen, afhandeling bedrijven en securitybedrijven. Onder het Platform is een Stuurgroep ingesteld, waarin vertegenwoordigers op directieniveau zitting hebben. Er zijn werkgroepen opgericht op het gebied van Terrorismebestrijding, Publieke Veiligheid en Openbare Orde, Grenscontrole, Vrachtcontrole, het Cameraproject en Innovatie en Technologie.

Nijhuis:

'Het BPVS levert ons veel op. Het is een directe, efficiënte manier van werken die voordelen heeft voor alle betrokkenen. Medewerkers kunnen doelmatiger worden ingezet en de capaciteit wordt beter benut. De camera's met hun ogen op afstand bieden belangrijke ondersteuning voor de processen. De 'return on investment' is goed. Dat is allemaal winst. Uiteindelijk moeten we op Schiphol de kosten scherp in de gaten houden willen we concurrerend blijven. Alleen zo houden we onze positie als Europe's preferred airport overeind.'

Concrete resultaten

Het BPVS heeft zich binnen korte tijd ontwikkeld tot een geaccepteerd en gerespecteerd gremium waar strategie en beleid van beveiliging en veiligheid gezamenlijk wordt aangepakt. Steeds met oog voor taken en verantwoordelijkheden van de onderscheidende partijen. Ook cultuurverandering is een belangrijk positief resultaat. Partijen gaan niet meer 'alleen voor zichzelf', maar er is een open cultuur gecreëerd waar gezamenlijke probleemstellingen leiden tot samen zoeken naar oplossingen die effectief en efficiënt zijn. Bij lopende zaken gaat het om risico beheersing en het wegnemen van knelpunten. Ook bij incidenten wordt gezamenlijk het beleid bepaald. De beheersorganisatie vertaalt zich in risicobeheersing. Zowel als het gaat om het naleven van wetten en regels, als het vertalen van nieuwe ontwikkelingen op het gebied van beveiliging of incidentafhandeling. Belangrijk is eveneens dat gezamenlijk een krachtige lobby kan worden gevoerd om geharmoniseerde, maar vooral ook werkbare maatregelen en middelen voor de beveiliging te kunnen inzetten.

Voorbeelden zijn:

- de Security Scan als voorbeeld van het initiatief van Schiphol om – als eerste luchthaven in de wereld – een middel te gebruiken dat personen kan onderzoeken zonder dat de privacy wordt aangetast. Inmiddels in de EU goedgekeurd en internationaal nagevolgd. Ook bij het vertalen van de wens om vloeistoffen in de handbagage vrij te geven, maar deze dan wel te controleren, vormt het gezamenlijk onderzoek naar detectie en 'false alarm' een bijdrage tot realistische en werkbare regelgeving.

- Het gezamenlijke cameraproject is eveneens uniek. In plaats dat elke partij zijn eigen camera's en dan naast elkaar zouden ophangen, wordt gebruik gemaakt van een gezamenlijke infrastructuur.Hierop worden bestaande- en nieuwe camera's op plekken waar deze nuttig en nodig zijn, opgehangen. Voldoende opslagcapaciteit zorgt ervoor dat in het geval van incidenten reconstructie mogelijk is. De uitvoering is zodanig dat iedere partij alleen maar die beelden kan zien waartoe hij is geautoriseerd. Met de camera's is een essentiële bijdrage geleverd aan taken van partijen met betrekking tot risicobeheersing, handhaving, controle en procesbeheersing.
- Een ander voorbeeld van een zeer goed resultaat is de ketenbenadering bij grens- en securityprocessen. Partijen zijn van elkaar afhankelijk voor de informatie van het passagiersaanbod per dag, per tijd en per filter. Hierop vanuit de ketengedachte zorgdragen voor voldoende inzet van capaciteit. Zowel wat betreft de techniek als de menskracht.
- Weer een andere belangrijke ontwikkeling is de zogenaamde Smartgate. Met dit one-stop controle concept worden uitgaande goederenstromen zoveel mogelijk gezamenlijk en in één keer gecontroleerd. De samenwerking is hier gebaseerd op informatie en een ketenaanpak, met als doel de druk op overheid te verminderen en kosten van alle partijen te verminderen, waardoor de rol van Nederland als distributieland ondersteund wordt.
- De toegangscontrole is verder ontwikkeld tot een hoog beveiligingsniveau. Persoonsgebonden kenmerken (biometrie) worden gebruikt om controles voor het betreden van beveiligde gebieden uit te voeren. Ook uitgaande medewerkers worden stelselmatig maar op onvoorspelbare momenten en plaatsen gecontroleerd.
- Ook communicatie heeft meer aandacht gekregen. Uitgangspunt is en blijft uiteraard het verstrekken van juiste informatie. Het afgewogen voorlichtings- en communicatiebeleid vertaalt zich in positieve zin, zowel structureel als na incidenten.

Nijhuis:

'We hebben samen in relatief korte tijd veel bereikt. Het is belangrijk dat we samen blijven optrekken en blijven zoeken naar manieren om dingen beter te doen. Natuurlijk heeft ieder zijn eigen verantwoordelijkheid, maar samen kunnen we security efficiënter en beter invullen. Dat blijkt uit de ervaringen met het BPVS.'

Toekomst

Het BPVS samenwerkingsmodel is een randvoorwaarde geworden voor samenwerking tussen partijen op Schiphol op beleidsniveau. De integrale aanpak levert niet alleen voor partijen zelf veel op aan effectiviteit en efficiency. Ook vanuit het buitenland blijkt dat met belangstelling en waardering naar de werkwijze van het BPVS wordt gekeken. Dit vertaalt zich in vertrouwen van de Nederlandse systematiek om beveiligings- en veiligheidsrisico's te beheersen.
Samen werken we voortdurend aan een beveiligingsniveau dat in combinatie met de dienstverlening de passagiers, de luchtvaartmaatschappijen en de overheden voor Schiphol doet kiezen.

Nijhuis:

'We staan aan de vooravond van grote investeringen. Beveiligingseisen nemen toe. Zo moeten vertrekkende en aankomende passagiers buiten het Schengengebied gescheiden worden. Ook daarbij werken we samen met alle partijen. Doel is steeds een optimale combinatie van voldoen aan beveiligingseisen en een goede dienstverlening aan de klant.'

drs. B.M.G. Janssen MCDM,
directeur Gezamenlijke Brandweer

Professionals in incidentbestrijding en dienstverlening

Hoe de brandweerzorg in de Rotterdamse Haven zich ontwikkelde tot een publiek private samenwerking

In de jaren '60 en '70 van de vorige eeuw ontwikkelde de Rotterdamse haven zich in hoog tempo in westelijke richting. Om de brandweerzorg te kunnen waarborgen richtten de gemeenten Rotterdam en Rozenburg de Intergemeentelijke Brandweer voor het Eiland van Rozenburg op (IBER). Vanuit de post Rozenburg werd uitgerukt naar alle industriële en openbare incidenten in het Botlek-, Europoort- en Maasvlakte gebied. Dit gebeurde met een basis beroepsbezetting ondersteund door de vrijwillige brandweerlieden uit Rozenburg. Daarnaast kregen zij steun vanaf de post Hoogvliet, die ook het gebied Pernis bediende Een 20-tal bedrijven had een bedrijfsbrandweer, waarvan de kwaliteit (kennis, ervaring en middelen) nogal verschilde.

Rond 1990 moest de overheidsbrandweer gaan voldoen aan de zorgnormen, waardoor er eigenlijk één of twee kazernes aan de sterkte moesten worden toegevoegd. Daarnaast moesten de bedrijven gaan voldoen aan de voorwaarden van het Besluit Bedrijfsbrandweren. Zowel de overheid als het bedrijfsleven moest investeren in het verbeteren van de brandweerzorg. Omdat bij beide partijen het idee ontstond dat een intensieve samenwerking een oplossing zou kunnen zijn, lieten zij een haalbaarheidsstudie uitvoeren. De uitkomst van de studie was dat samenwerking minder meerkosten zou geven en het kwaliteitsniveau van de dienstverlening zou verhogen. De vorming van één gezamenlijk korps zou de kwaliteit ten goede komen en tevens zou het maken van afspraken met 35 bedrijfsbrandweren niet meer nodig zijn.

Intensief bestuurlijk overleg tussen de Commandant Brandweer, Directeur Havenbedrijf en enkele keyplayers uit het bedrijfsleven leidde in 1997 tot de oprichting van de juridische entiteit "Openbaar Lichaam Gezamenlijke Brandweer" (OLGB). Hierin participeerden de gemeenten Rotterdam en Rozenburg met een door de bedrijven opgerichte "Coöperatie van Industriële Bedrijven met een Uitgesloten Aansprakelijkheid" (CIBUA). Namens de overheid zaten de Burgemeesters van Rotterdam (voorzitter) en Rozenburg en de Wethouder Haven in het bestuur van het OLGB. De CIBUA wordt vertegenwoordigd door drie bestuursleden, waaronder één secretaris/penningmeester. Wegens opheffen van de gemeente Rozenburg in maart 2011 maakt de burgemeester van die gemeente geen deel meer uit van het bestuur.
De Gezamenlijke Brandweer (GB) voert de preparatieve en repressieve taken uit, terwijl de preventietaken bij de Rotterdamse Brandweer bleven (nu Veiligheidsregio Rotterdam-Rijnmond/VRR).

Op grond van de uitkomsten van de haalbaarheidsstudie werd de financiële verdeling bepaald op 27% voor de overheid en 73% voor de CIBUA. Deze verdeelsleutel is regelmatig onderwerp van discussie, maar de balans in deze verdeelsleutel blijkt een belangrijk criterium te zijn voor de continuïteit van deze PPS. De financiële verdeling tussen de bedrijven vindt plaats op grond van de door de overheid conform artikel 13 Brandweerwet (nu art 31 Wet Veiligheidsregio's) aangewezen aantal medewerkers voor hun bedrijfsbrandweer. Momenteel heeft één bedrijf een eigen brandweer en hebben de vier raffinaderijen de helft van hun aanwijzing uitbesteed aan het OLGB.

In 1997 is men begonnen met de bouw van drie nieuwe kazernes, de verbouwing van een gebouw tot kazerne en de inrichting van een tijdelijke post in Pernis. Daarnaast moest personeel geworven en getraind worden (afkomstig vanuit de bedrijven en de omringende meestal vrijwillige korpsen). Verder werd veelal tweedehands en soms zeer oud materieel aangeschaft.

Vanaf 2 januari 1998 is de Gezamenlijke Brandweer (GB) operationeel vanuit 5 beroepsposten met 30 personen rond de klok in een 3-ploegendienst en een vrijwillige eenheid in Rozenburg. Bij grote incidenten zorgen de vrijwilligers ook voor de herbezetting. De GB wordt jaarlijks circa 1000 maal opgeroepen voor diverse incidenten, zowel op bedrijfsterreinen als op openbaar gebied. Om de lijn met het bevoegd gezag te waarborgen hebben alle leidinggevenden tevens een onbezoldigde aanstelling bij de brandweer Rotterdam-Rijnmond (nu VRR).

In 2003 heeft de gemeente Rotterdam, als gevolg van bezuinigingen, de brandweerzorg van de deelgemeente Hoogvliet en de wijk Pernis overgedragen aan het OLGB. Hiermee is de verdeling van financiën gewijzigd in 34,1% voor de overheid en 65,9% voor de CIBUA. Als gevolg hiervan heeft de GB ook in Hoogvliet een vrijwillige brandweer opgericht.

De GB rukt in principe uit met een standaardeenheid (Combinatie eenheid = CE) Deze CE bestaat uit een industriële autospuit groot vermogen (met 4 m^3 schuimvormend middel (SVM) en veel slangen) en een tankautospuit (TS) (met hoge en lage drukpomp en technisch hulpverleningsgereedschap). Voor vijf eenheden zijn deze functies in één voertuig samengebracht. De eenheid wordt bezet door een bevelvoerder met 5 manschappen. Voor industriële branden worden in regel ook haakarmbakken met ieder 10 ton SVM mee gealarmeerd.

Vanaf het begin heeft de GB de doelstelling gehad om geld te verdienen met de "beschikbaarheidsnuttigheid" van het operationele personeel in de stille uren. Echter door de groei van het aantal van 42 bedrijven in 1998 naar 61 bedrijven nu is er door de forse toename van de oefenuren van stille uren geen sprake meer. Momenteel worden vooral activiteiten uitgevoerd voor de eigen organisatie, de VRR en de ledenbedrijven. Dit betreft:

- het exploiteren van een hoog gekwalificeerde werkplaats voor het onderhoud van persoonlijke beschermingsmiddelen en brandslangen;
- de in- en verkoop van SVM voor de eigen organisatie en de leden bedrijven (standaardisatie);
- de verhuur van brandwachten;
- het leveren van consultancy;
- en het geven van diverse trainingen op locatie en op het eigen trainingscentrum.

Binnen de GB hebben zich diverse specialismen ontwikkeld. Alle operationele medewerkers zijn opgeleid en getraind in het werken in gaspak. Per 1 januari 2012 voert de GB ook de gaspakkentaak binnen de regio uit voor de VRR. Hier hoort ook de eigen ontsmettingseenheid en de ondersteuning van het CBRN peloton bij. Eén van de specialismen is de COBRA, een hoge druk blus-

systeem, dat regelmatig is ingezet bij incidenten in de industrie, maar ook bij woningbranden. Deze medewerkers bedienen ook het schuimblusvoertuig, dat samen met de VRR wordt geëxploiteerd. Een eenheid levert het specialisme hoogte- en diepteredding door middel van een gecertificeerd hoogtereddingsteam (HRT) gefinancierd door 18 ledenbedrijven. Deze bedrijven hebben een verhoogd risico op hoogte of diepte incidenten. Voor de inzet in de regio draagt de VRR hieraan ongeveer 25% bij. Op verzoek en gefinancierd door Rijkswaterstaat levert de GB in samenwerking met een team van de VRR een team scheepsbrandbestrijding voor incidenten op de Noordzee. De GB voert ook uitvoerende werkzaamheden uit voor de Stichting Schermenpool, een samenwerking tussen bedrijven en het Havenbedrijf van Rotterdam ter bestrijding van verontreiniging van oppervlaktewater in de haven.

Op basis van de milieuwetgeving is in 2006 door de DCMR, Brandweer Rotterdam-Rijnmond, Deltalinqs en de betrokken bedrijven besloten tot de oprichting van de Industriële Brandbestrijding Pool (IBP) met als doel de aanschaf, het beheer, de training en de bediening van grootschalig materieel voor het blussen van grote tankbranden (tot 89 meter doorsnee). De investering is gedaan door de bedrijven en de middelen worden beheerd en bediend door de GB met ondersteuning van eenheden van de VRR en het Havenbedrijf. Het systeem levert op een afstand van ruim 100 meter en ruim 22 meter hoog 80 kubieke meter blusschuim per minuut. De totale mobiele voorraad SVM bedraagt circa 200 ton. In de loop van dit jaar wordt het systeem uitgebreid met materieel voor de bestrijding van tankputbranden.

In december 2011 is de nieuwe kazerne Butaanweg op het Beneluxplein in gebruik genomen. Deze kazerne bedient het industriegebied Pernis, de wijk Pernis en een deel van de deelgemeente Hoogvliet. Door de expansie van de Rotterdamse haven richting zee gaat de GB voor de gemeente en de bedrijven ook de brandweerzorg leveren op de tweede Maasvlakte. Hiertoe wordt momenteel een nieuwe kazerne gebouwd en worden 27 personeelsleden geworven, opgeleid en getraind. De kazerne zal op 1 september 2012 operationeel zijn. Vanaf dat moment heeft de Gezamenlijk Brandweer circa 285 personen (inclusief 60 vrijwilligers) in dienst.

De GB is als Publiek Private Samenwerking (PPS) niet meer weg te denken uit het Rotterdamse havengebied, mede omdat er sprake is van een hogere kwaliteit van de incidentenbestrijding tegen minder meer kosten. Zij wordt onder meer door het Havenbedrijf als één van de sellingpoints gebruikt bij de werving van nieuwe bedrijven voor het havengebied. Dit alles onder het missie statement “Professionals in incidentbestrijding en dienstverlening”

De Nederlandse veiligheidsbranche is de landelijke branchevereniging van de particuliere beveiligingsbedrijven. De branche vertegenwoordigt 90% van de omzet en 31.500 beveiligers. De branche heeft de afgelopen decennia een aanzienlijke groei doorgemaakt en heeft zich ontwikkeld tot een professionele partner in de veiligheidsketen. De overheid maakt steeds beter gebruik van de meerwaarde die de veiligheidsbranche te bieden heeft. Speerpunt van de branche de komende jaren is door bredere samenwerking met de overheid op lokaal en nationaal niveau een wezenlijke bijdrage te leveren aan de veiligheid in Nederland.

mr. Laetitia Griffith,
voorzitter Nederlandse Veiligheidsbranche

De Nederlandse **veiligheidsbranche: partner** in de **veiligheidsketen!**

De particuliere veiligheidsbranche is sinds eind jaren '80 van de vorige eeuw sterk gegroeid, zowel in omvang als in professionaliteit. Naast particuliere beveiliging en bedrijfsrecherche worden ook particuliere alarmcentrales, geld- en waardetransport en evenementenbeveiliging tot de sector gerekend. Er is een wettelijk vergunningensysteem geïntroduceerd dat eisen stelt aan vakbekwaamheid en betrouwbaarheid van de in te zetten personen. Voor alle beveiligers is er een verplichte opleiding. En tewerkstelling vindt niet eerder plaats dan na een screening door de politie op criminele antecedenten. Deze screening wordt iedere drie jaar herhaald. Op het gebied van zelfregulering heeft de branchevereniging de nodige stappen gezet. Er zijn gedragscodes, er is een beroepscommissie die bemiddelt bij geschillen en er zijn sinds 2006 verschillende kwaliteitskeurmerken.

Cruciale werkterreinen

Beveiligers zijn werkzaam in winkels, scholen, kantoren, ziekenhuizen en gevangenissen. Zij surveilleren op bedrijventerreinen, industriële complexen en in woonwijken. Zij worden voorts ingezet als toezichthouders en handhavers in het publieke domein of als bijzondere opsporingsambtenaren (boa's) in dienst van de gemeente. Door middel van moderne communicatiemiddelen en technieken staan medewerkers in rechtstreekse verbinding met particuliere alarmcentrales. Onderstaand worden enkele werkterreinen uitgediept.

Luchthavens

Vele duizenden beveiligers leveren op Schiphol en de andere luchthavens een bijdrage aan de veiligheid en het voorkomen van terrorisme. Ze hebben daarbij niet alleen een rol bij het controleren van de passagiersstromen maar ook bij cargo security en de fysieke beveiliging van de buitenterreinen. De inzet vindt doorgaans plaats onder operationele regie – en toezicht van de Marechaussee.

Zeehavens

In de zeehavens zijn gespecialiseerde beveiligers betrokken bij de controles op lading, containers en de fysieke veiligheid op de terminals. Ze staan in contact met Port Security Officers en de terminals en zijn betrokken bij nood- en rampenplannen en het Port Security Facility Plan. In het zogenaamde Oog & Oor project wisselen de zeehavenpolitie en beveiligingsbedrijven gegevens uit over verdachte situaties en kentekens.

Vitale infrastructuur

Private veiligheidsprofessionals zijn ook werkzaam bij sectoren die vallen onder de vitale infrastructuur, zoals energiecentrales, installaties in de chemische industrie en sectoren verantwoordelijk voor drinkwater, gas en brandstoffen. Deze beveiligers of brandwachten die ook hun beveiligingsdiploma hebben gehaald, zijn de ogen en oren voor de security managers van de locaties. Vaak zijn zij als eerste ter plaatse bij incidenten. Hun meerwaarde is gelegen in hun expertise als veiligheids-adviseur en preventieadviseur.

Samenwerking en informatie-uitwisseling

Samenwerking en informatie-uitwisseling tussen beveiliging en politie zijn steeds vaker de norm. Efficiënte samenwerking tussen de particuliere beveiliging, de gemeente en de politie draagt bij aan de veiligheid. Een goed voorbeeld vormen de regionale toezichtruimten in een drietal politieregio's (Stichting Criminee!). Politiefunctionarissen en observanten van particuliere bedrijven lezen hier gezamenlijk camera-beelden uit. Het is al geruime tijd mogelijk voor de politie om informatie uit te wisselen over onder meer verdachte voertuigen, gezochte kentekens en signale-menten. Zo werd onlangs in de regio Twente een convenant gesloten tussen het politiekorps en drie bedrijven met een keurmerk Beveiliging. Het gaat daarbij om tweerichtingsverkeer van informatie-uitwisseling. Privacybelangen van betrokken personen worden geborgd door vooraf duidelijke afspraken te maken over hoe er met uitgewisselde informatie wordt omgegaan.

Belangrijke schakel

De particuliere beveiliging vormt vanwege zijn infor-matiepositie op cruciale werkterreinen anno 2012 een belangrijke schakel in de nationale veiligheid. Expertise van de branche kan helpen bij de preventie en het beheersen van een crisis. Beveiligers beschikken over specifieke en doelgerichte informatie. Bij rampen en crises – op nationaal, regionaal en lokaal niveau – is het zaak dat die informatie snel beschikbaar is. Betrokkenheid van de branche en informatie-uit-wis-seling is daarom van essentieel belang bij zowel de totstandkoming van (gemeentelijke) veiligheids-plannen als bij crisisbeheersing en rampenbestrijding. Met als doel een veiliger Nederland!

Nikki Jansweijer en Marloes Smelter,
programma Dreigingen en Capaciteiten, directie Nationale Veiligheid, Nationaal Coördinator Terrorismebestrijding en Veiligheid

"Een beetje crisis helpt wel"
Business Continuity Management **bij ABN AMRO**

In het kader van het thema Publiek private samenwerking sprak het Magazine met Johan van Hall, Chief Operating Officer en lid van de Raad van Bestuur bij ABN AMRO over Business Continuity Management (BCM), over continuïteitsverstoringen, het belang van oefenen en de inrichting van een effectieve crisismanagement organisatie.

Johan van Hall

Business Continuity Management

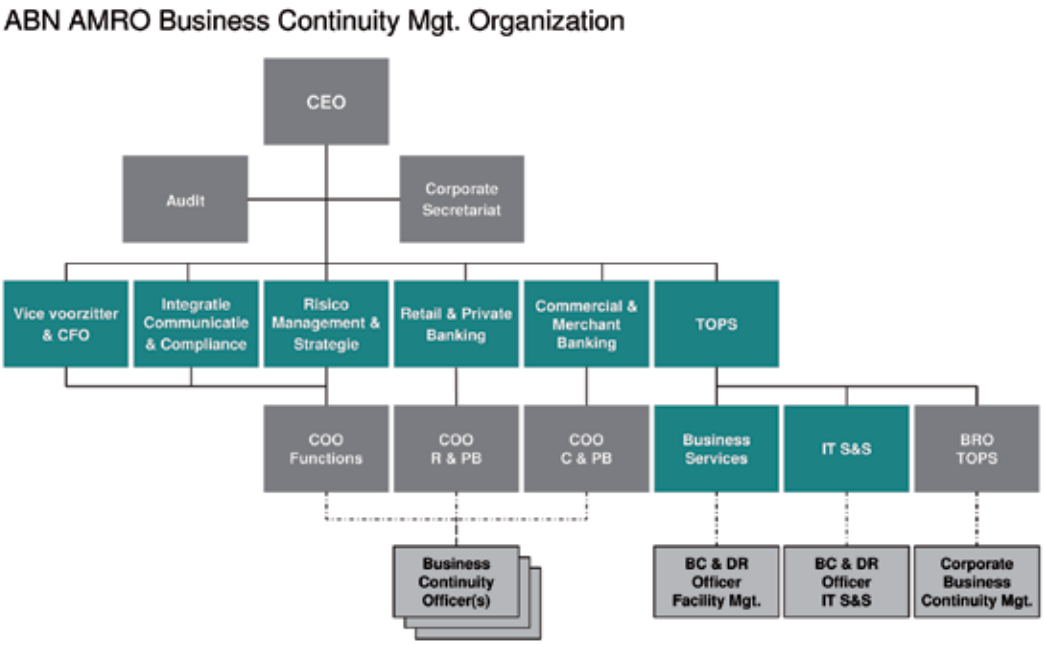
De heer Van Hall wil graag beginnen met te vertellen waaróm bij ABN AMRO veel aandacht wordt besteed aan Business Continuity Management (verder BCM). De bank heeft allereerst een verantwoordelijkheid richting haar klanten. Bij verstoringen in de dienstverlening zijn de gevolgen vérstrekkend. Klanten kunnen dan bijvoorbeeld geen betalingen verrichten of ontvangen. Een dergelijke continuïteitsverstoring kan zelfs leiden tot maatschappelijke ontwrichting. De belangrijkste motivatie voor BCM is dan ook de maatschappelijke verantwoordelijkheid van de organisatie. Daarnaast heeft het bedrijf natuurlijk een verantwoordelijkheid naar haar werknemers en is het verplicht om te voldoen aan regelgeving op dit gebied.

BCM is in alle bedrijfsonderdelen van ABN AMRO verankerd. Om ondersteuning te verzorgen is er een speciaal Competence Centre BCM ingericht. Hier werken vijf mensen full-time aan BCM. Zij schrijven frameworks voor handboeken, plannen oefeningen en opleidingen, monitoren de kwaliteit van de plannen, houden telefoonlijsten bij etc. Doordat zij een ondersteunende, aanjagende én monitorende rol vervullen, blijft BCM binnen de gehele organisatie hoog op de agenda en wordt de kennis over BCM geborgd. Het Competence Centre rapporteert via de Business Risk Officer TOPS aan de Chief Operating Officer (COO), dus de Raad van Bestuur.

Als zich een incident of crisis voordoet wordt het Crisis Management Team (CMT) in werking gesteld. Om snel te kunnen reageren heeft het CMT een uitvoerende bevoegdheid buiten de reguliere lijn om. Afhankelijk van de zwaarte en het soort probleem worden de leden van het CMT bepaald. Bij een code zwart (de zwaarste categorie) zit de COO het CMT voor. Communicatie is vast vertegenwoordigd in het team, verder kan de bezetting verschillen, afhankelijk van het soort incident. Zo heeft tijdens de opschaling in 2009 voor de grieppandemie de ARBO arts deelgenomen in het CMT. Om de slagkracht te vergroten bestaat het CMT altijd uit een mix van experts en beslissers. Op deze manier kan het CMT direct handelen op basis van de door de experts verstrekte kennis en informatie. De heer Van Hall benadrukt verder dat voor een adequaat crisismanagement de medewerkers een aantal belangrijke competenties moeten hebben. Hij noemt dit de "vijf C's". Medewerkers zijn competent (je moet echt weten hoe het zit wil je een crisis analyseren en oplossen), committed (bedrijf is in problemen en we zullen dat snel oplossen qua houding), coöperatief (sámen is de sleutel, buiten de reguliere lijn om), creatief (de situatie vraagt om niet-standaardoplossingen, maar welke) en communicatief (hoe moeilijk ook maar tijdens de crisis frequent blijven communiceren met interne en externe stakeholders is key).

Kwetsbaarheden, afhankelijkheden en maatregelen

De organisatie is voor haar dienstverlening mede afhankelijk van andere (interbancaire) instellingen. Met deze instellingen zijn contracten en 'Service Level



Agreements (SLA's) afgesloten waarin afspraken zijn gemaakt om het risico op verstoring van de continuïteit te verkleinen.
Verder probeert ABN AMRO zo onafhankelijk mogelijk te zijn. Hiertoe zijn voor verschillende scenario's voorbereidende plannen gemaakt en maatregelen genomen. Zo zijn er bijvoorbeeld noodstroom voorzieningen voor de kritieke systemen en zijn er uitwijklocaties ingericht voor kritieke processen. In de plannen is uitgewerkt hoe, wanneer en door wie deze noodvoorzieningen in gebruik genomen moeten worden.
Een belangrijke voorwaarde voor het slagen van het BCM beleid is dat dit soort voorbereidingen en maatregelen is ingeslepen in de cultuur van de organisatie. De heer Van Hall benadrukt daarbij wel dat de voorbereidingen ergens ophouden. Het is onmogelijk om overal rekening mee te houden. In onvoorziene situaties moet je daarom kunnen vertrouwen op een competente crisisorganisatie.

Publiek private samenwerking

In het kader van het vitale infrastructuurbeleid van de overheid werkt ook ABN AMRO samen met publieke en private partners. De bank neemt haar maatschappelijke verantwoordelijkheid voor de continuïteit van het betalings- en effectenverkeer en neemt als financiële instelling deel aan overleg en samenwerking tussen overheid en vitale sectoren. Daarnaast is ABN AMRO aangesloten op het Alerteringssysteem Terrorismebestrijding. Door dit soort strategische samenwerkingsverbanden wordt de weerbaarheid tegen maatschappelijke ontwrichting versterkt. Een bijkomend voordeel van deze samenwerkingsverbanden zijn de best-practices en ervaringen die de organisaties met elkaar delen.

Oefeningen

Het Competence Centre heeft voor alle organisatieonderdelen een uitgebreid oefenschema opgesteld. De meeste onderdelen worden minimaal eens per jaar officieel beoefend. Dit zijn veelal theoretische oefeningen, georganiseerd aan de hand van een realistisch scenario. De leden van het CMT oefenen ook hun communicatievaardigheden. Naast deze geplande oefeningen vinden er jaarlijks genoeg incidenten (groot en klein) plaats, waarbij alle plannen in de praktijk worden getoetst. "Een beetje crisis helpt wel voor een adequaat BCM" merkt de heer Van Hall op. Voorbeelden van recente incidenten zijn stroomstoringen, brand en de bijbehorende ontruiming van een kantoorpand in Londen, de tsunami in Japan [ABN AMRO heeft Japanse klanten en ook medewerkers gestationeerd in Japan, red.], uitval van servers van een rekencentrum en problemen met betalingsverkeer na abusievelijk dubbele aanlevering/verwerking transactiebatch.
Na elke oefening of crisis volgt een formele evaluatie waarin zowel naar de samenwerking als de inhoud wordt gekeken en de verbeterpunten die uit de evaluaties volgen worden vervolgens nadrukkelijk gemonitord door het Competence Center.

Tot slot

Op de vraag wat volgens de heer Van Hall de belangrijkste voorwaarde is voor een degelijk en effectief BCM antwoordt hij vrijwel direct dat het belangrijk is de administratieve organisatie goed neer te zetten, maar het daarna vooral ook te gaan dóen. "Papier is geduldig, maar uiteindelijk gaat het om goed getrainde mensen" aldus Van Hall.

Hulp aan de hulpverleners

De samenleving verandert. Het politieke beleid verandert. Ook de hulpverlening verandert. Duidelijk is inmiddels dat de rol van de professionele hulpverleningsdiensten mee verandert. Brandweer, politie en de ambulancediensten staan voortdurend onder druk van de politiek om efficiënter te werken. De rol van de hulpverleningsdiensten ten aanzien van het optreden bij grootschalige incidenten wordt opnieuw bekeken.

Jan Wolter Ouwehand,
directeur Nederland Instituut voor Bedrijfshulpverlening (NIBHV)

De overheid is inmiddels tot het besef gekomen dat zij de veiligheid en de daarbij behorende hulpverlening aan burgers niet voor 100% kan garanderen. Het zelf regelen door burgers van zaken die vroeger als vanzelfsprekend door de overheid werden geregeld, komt nu meer op het bordje van de mensen zelf te liggen. De overheid kan ook niet alles regelen, de burger moet zich

hier steeds meer bewust van worden en haar eigen verantwoordelijkheid nemen.
Hoe moet het nu verder met de 'veiligheid'? Op dit moment wordt uitgebreid door de politiek en betrokkenen gesproken over zelfredzaamheid.
Zelfredzaamheid is het vermogen van organisaties en groepen of individuen om zichzelf te redden uit gevaarlijke of bedreigende situaties. Vroeger werd gedacht dat de hulpverleningsdiensten hier garant voor stonden. Een achterhaalde gedachte. De capaciteit is niet voldoende om bij grootschalige gebeurtenissen overal en met voldoende hulpverleners en hulpmiddelen aanwezig te zijn. Maar zo somber is de situatie in ons land zeker niet. In Nederland leven wij in een zeer veilige omgeving.

Uit diverse onderzoeken blijkt dat burgers veel meer zelf kunnen en ook daadwerkelijk doen in noodsituaties en daarbij medeslachtoffers bijstaan en helpen.
Zelfredzaamheid is altijd en overal aanwezig. Anderen helpen zit bij iedereen in zijn aard. Dit blijkt als we wat getallen op een rij zetten. Het aantal professionele hulpverleners, werkzaam bij de brandweer, politie en ambulancediensten bedraagt in totaal ongeveer 75.000 personen. Niet veel als je bedenkt dat er in Nederland bijna 17 miljoen mensen wonen. Een snelle rekensom laat echter zien dat er in Nederland veel mensen zijn die zich 'vrijwillig' bezighouden met veiligheid en hulpverlening.

Het aantal EHBO'ers met een geldig diploma bedraagt ongeveer 250.000. Allemaal met kennis en vaardigheden om eerste hulp te verlenen aan de medemens in noodsituaties. Binnen bedrijven moet bovendien de bedrijfshulpverlening zijn geregeld. Daarbij is een groot aantal bedrijfshulpverleners actief. Deze bedrijfshulpverleners zijn getraind om niet alleen eerste hulp te verzorgen, maar ook om beginnende branden te blussen en ontruimingen en evacuaties zelfstandig uit te voeren. Samen met de EHBO'ers kunnen we uitgaan van een totaal van ongeveer 750.000 extra 'vrijwillige' hulpverleners. Daarmee is er sprake van een substantieel aantal dat altijd en overal aanwezig is. Niet alleen tijdens werkuren, maar 7 dagen per week en 24 uur per dag.

Een optimale hulpverlening kan worden bereikt als de professionele en niet-professionele hulpverlening elkaar weten te vinden. Wat missen we daar op dit moment nog voor? Ik denk duidelijkheid over wat we van elkaar kunnen verwachten en hoe we elkaar kunnen bijstaan. Als dat helder is, kan dit worden meegenomen in de voorlichting, scholing en training. De eerste stappen zijn al gezet om te komen tot een goede afstemming en samenwerking tussen de 'vrijwillige' en professionele hulpverleners. Een goede uitwerking van deze samenwerking is van cruciaal belang voor de veiligheid in Nederland.

Mw drs. Gonne Schras,
senior adviseur bureau In-pact,
landelijk programmamanager Burgernet

Burgernet werkt!

"Alle verwachtingen en prognoses rond de uitrol van Burgernet zijn overtroffen, Burgernet werkt!" Dit zei minister Opstelten van Veiligheid en Justitie op 12 december 2011 bij het in ontvangst nemen van de eindrapportage Burgernet in Utrecht. Inmiddels heeft Burgernet ruim 700.000 deelnemers en is Burgernet operationeel in circa 280 gemeenten.

Het idee achter Burgernet

Burgernet is een voorbeeld van een bijzondere vorm van burgerparticipatie. In 2004 werd in Nieuwegein door de politie in nauwe samenwerking met de gemeente een uniek experiment opgezet met de bedoeling burgers meer te betrekken en te laten bijdragen aan de veiligheid in hun omgeving. Burgers kunnen zich opgeven als deelnemers aan een telefonisch/communicatie informatienetwerk. Via de (mobiele) telefoon krijgen deelnemers van de centralist van de meldkamer een gesproken bericht of een tekstbericht per SMS of E-mail met het verzoek uit te kijken naar een vermist kind, inbreker of gestolen auto. Deelnemers kunnen dan rechtstreeks en kosteloos terugbellen als ze wat hebben gezien. De politie kan daardoor sneller en meer gericht in actie komen. Na afloop krijgen alle bereikte deelnemers een bericht over het resultaat. Daarnaast wordt de actie geplaatst op de publieke website www.burgernet.nl.

Deze aanpak is zo succesvol gebleken dat de toenmalige ministers van BZK en Justitie, het programma Burgernet de opdracht verstrekten om het concept landelijk te gaan uitrollen. Als doelstelling voor landelijke invoering werd geformuleerd dat alle meldkamers werden aangesloten op Burgernet en dat er een samenwerking tot stand moest komen met minimaal 50 gemeenten. Deze doelstelling is glansrijk gehaald. Inmiddels heeft Burgernet ruim 700.000 deelnemers en is operationeel in circa 280 gemeenten.

Doorontwikkeling concept Burgernet

De focus van het programma Burgernet lag gedurende de eerste fase op betrekken en opsporen. Op initiatief van de korpsen en gemeenten is de toepassing van Burgernet verbreed. Naast opsporen wordt Burgernet nu ook ingezet om te informeren en te alarmeren. In de reeks informeren, betrekken, alarmeren en opsporen is naast een gradatie naar de mate van spoed (toenemend van links naar rechts) ook de gewenste relatie tussen overheid en burgers zichtbaar. Van in de breedte 'informeren' tot en met gericht, voor één concreet incident, direct hulp vragen bij het 'opsporen'. Niet tijdkritische berichten worden vaak via andere kanalen dan de meldkamer verzonden. Met name de berichten met als doel informeren worden door de gemeenten verspreid.

Informeren	Betrekken	Alarmeren	Opsporen
• Preventie • Veiligheid • Zwemwater / volksgezondheid • Wegafsluiting • Bosbrandgevaar	• Weggelopen kind • Incident in wijk • Woninginbraken • Leefbaarheid • Veiligheid • Etc.	• Bom • Gaslek • Explosie / aanslag • Rampen • Etc.	• Overvaller • Woninginbreker • Persoon vermist • Gestolen voertuig • Etc.

Operationele resultaten

Maandelijks worden circa 400 Burgernetacties in gang gezet. Aan een actie nemen gemiddeld 1300 Burgernet-deelnemers deel. Ongeveer 60 procent van de acties heeft een tijdkritisch karakter. In 10 procent van de gevallen kan dankzij informatie van Burgernetdeel-nemers een verdachte worden aangehouden of een vermiste worden getraceerd. Daar komt nog bij dat circa 40 procent van de Burgernetacties een meer indirecte, maar zeker ook waardevolle bijdrage heeft aan het opsporingsproces. De positieve resultaten leiden, naast het vergroten van de veiligheid van de samenleving, tot een aanzienlijke kostenbesparing. Het achteraf rechercheren vraagt vele uren aan recherchecapaciteit die uiteindelijk minder opleveren. Daarnaast blijkt uit onderzoek dat Burgernet deelnemers meer vertrouwen hebben in de overheid.

Inbedding Nationale Politie

Het jaar 2012 is een overgangsjaar waarin Burgernet ingebed wordt in de Nationale Politie. Naast de inbedding heeft het programma de doelstelling gekregen dat Burgernet is uitgerold in ten minste 300 gemeenten en er minimaal 800.000 burgers actief bij Burgernet betrokken zijn, een doelstelling die al bijna is gerealiseerd. Het huidige programmabureau Burgernet blijft ook in 2012 verantwoordelijk voor de realisatie van de doelstellingen.

Foto: Peter Monteny (Politie Haaglanden)

Foto: Fons Sluiter Fotografie en Norbert Waalboer Fotografie

In Denemarken is het grootste deel van de brandweerzorg privaat georganiseerd. De grootste private aanbieder is Falck, die de brandweerzorg uitvoert in ruim tweederde van de Deense gemeenten. Het scenario is in alle landen hetzelfde: er breekt brand uit of er gebeurt een ongeval, het alarm gaat af bij de brandweer en de brandweer rukt uit. De opgave is in elk land hetzelfde, het incident dient snel en doeltreffend te worwden bestreden. In tegenstelling tot bijvoorbeeld Nederland is het merendeel van de brandweerlieden in Denemarken aangesteld bij een private onderneming, in dit geval Falck. Het betreft een Deens bedrijf dat veiligheids- en gezondheidsdiensten levert. Hieronder vallen wegenwacht, ARBO-diensten, trainingen, amulancediensten voor 80% van de Deense bevolking en de brandweerzorg in ruim tweederde van de gemeenten. Het grootste deel van de brandweerlieden bij Falck heeft een vrijwilliger dienstverband.

Brandbestrijding op zijn Deens

Ivonne Couwenberg,
directeur Blomberg Instituut [1]

Knud Børge Møller is gemeentelijk brandweercommandant in Hjørring, een gemeente in het noorden van Denemarken. Hij maakt gebruik van de diensten van de brandweer van eerdergenoemd bedrijf. “Denemarken is opgedeeld in 98 gemeenten, die zelf de keus maken of ze hun brandweerzorg publiek of privaat organiseren of een combinatie hiervan. Verder zijn er tegen de grens met Duitsland nog een aantal op Duitse leest geschoeide brandweren. En ook al is de leverancier van de brandweerzorg privaat, de samenwerking tussen de gemeenten en het bedrijf is hecht. De werkzaamheden worden in goede afstemming uitgevoerd”, aldus Møller. De gemeente blijft verantwoordelijk voor een snelle en adequate hulpverlening, ook al zorgt de private leverancier voor de brandweervoertuigen en het materieel, de bemensing, de opleidingen en oefeningen, de verbindingsmiddelen etc.
In Hjørring levert Falck haar diensten vanuit vier brandweerkazernes. Møller legt uit, dat de sterkte van de brandweer wordt gebaseerd op een gemeentelijke risico-analyse. De brandweercommandant maakt een voorstel voor het college en de gemeenteraad, zodat de politiek uiteindelijk het serviceniveau in de gemeente bepaalt. De gemeente is dus verantwoordelijk voor het aantal brandweerlieden, voertuigen etc. Vanuit het Ministerie van Defensie, waaronder de brandweer valt, wordt slechts op hoofdlijnen de dimensionering bepaald.
De bestuurlijke leiding van de brandweer is binnen de gemeente neergelegd bij de commissie ‘hulpverlening’, waarvan de burgermeester de voorzitter is en de brandweercommandant de secretaris. Verder hebben onder andere drie gemeenteraadsleden en de politiechef zitting in de commissie. Een vertegenwoordiger van de private brandweer is vaak agendalid. In deze commissie worden alle brandweerzaken behandeld, voordat deze worden doorgeleid naar het college en de gemeenteraad. Møller ziet het bedrijf als een competente en betrouwbare sparringpartner. Doordat ze een grote leverancier van brandweerzorg in Denemarken zijn, leveren ze ook een flinke bijdrage aan nieuwe en doeltreffende oplossingen voor de brandweerzorg. “Veel innovatieve oplossingen zijn het resultaat van een hechte en constructieve samenwerking tussen de private aanbieder en de gemeente” besluit Møller zijn verhaal.

[1] Dit artikel is geschreven op basis van interviews als verdieping op de Bestuurlijke Veiligheidsdialoog van 10 november 2011, waar Knud Borge Møller, gemeentelijk brandweercommandant in Hjørring, te gast was en sprak met bestuurders uit het OOV-domein over publiek private samenwerking in de brandweerzorg.

De politieke samenwerking

Sinds 1926 hebben private ondernemingen de mogelijkheid om brandweerzorg te leveren, toen de toenmalige sociaal-democratische regering dit bij wet mogelijk maakte. De gemeente Ishøj ligt ten zuiden van Kopenhagen en is een van de gemeenten waar Falck de brandweerzorg levert. De sociaal-democratische (gekozen) burgemeester Ole Bjørstorp staat aan het hoofd van deze 21.000 inwoner tellende gemeente. Bjørstorp onderscheidt drie hoofdredenen waarom de gemeente heeft gekozen voor een private leverancier van de brandweerzorg.

Ten eerste de zekerheid en continuïteit van de levering van de brandweerwerkzaamheden. Het bedrijf is een zeer grote organisatie die zijn contractafspraken nakomt. Een paar jaar geleden was er 's nachts brand in de brandweerkazerne in een stadje in Jutland. De hele kazerne brandde tot de grond toe af met alle inventaris. De volgende ochtend al, was de brandweer weer compleet uitgerust met brandweervoertuigen, materieel, uitrukkleding voor de brandweerlieden etc. Het enige wat nog ontbrak was de brandweerkazerne. Dat kan alleen een grote organisatie.

De tweede reden zijn de kosten. Meerdere onderzoeken laten zien dat private brandweerzorg goedkoper is, omdat een grote organisatie schaalvoordelen heeft op onder andere het gebied van inkoop en door de combinatie van taken. Tegelijkertijd geeft een contract met vaste jaarlijkse kosten voor de gemeenten budgetzekerheid en dus geen onaangename financiële verassingen.

De derde reden is kwaliteit. De brandweer van Falck is de enige brandweer in Denemarken die ISO 9000 gecertificeerd is. "De gemeente Gentofte ten noorden van Kopenhagen, die in 2009 de brandweerzorg uitbesteedde, laat zien dat er veel geld te besparen is. Hier heeft de gemeente zelf berekend dat zij met hun tienjarig contract 40 miljoen Deense kronen (7 miljoen euro) besparen. Bijna 20% van de oorspronkelijke begroting", zegt Bjørstorp.

Als de brandweer, net als in Gentofte, overgaat van publiek naar privaat dan zijn er in Denemarken vaste regels voor de overgang van het personeel. De private partij is hierbij verplicht om het zittende brandweer-

Fire fighting operation
private , public and volunteer provision

- Red = Falck
- Green= Municipal
- Grey = Volunteer
- Other colours= mixed or other providers

Fire stations

	Stations	Auxiliary Stations
Falck	113	24
Municipal	80	14
Volunteer	41	23
Others	10	1

Fire Vehicles (manned) 1761

About 40.000 turn-outs a year
(false alarm about one third of turnouts)

Source:
Danish Emergency Management Board

personeel een contract aan te bieden. De brandweerlieden zijn vrij om op dit aanbod in te gaan. In Gentofte koos 80% van het brandweerpersoneel er voor om over te stappen naar Falck.

Brandweerman John Hammer van de brandweer in Gentofte, die in eerste instantie een fel tegenstander was van de overgang van de brandweerzorg naar een private partij, constateert een kleine twee jaar later: “ik moet toegeven dat we zeer goed zijn ontvangen. Mijn werkplezier is juist gestegen ten opzichte van mijn vorige werkgever. Als ik de resultaten van de overgang samenvat, dan heeft de overgang van publiek naar privaat in ons geval geleid tot meer focus op het inhoudelijke werk, meer aandacht voor aansturing van het personeel en een toenemende focus op kwaliteit van zowel de oefeningen als de uitruk”.

Goede resultaten

Uit de ‘Brandweerstatistiek 2011’ van het Deense Centraal Bureau voor de Statistiek blijkt dat Falck snelle uitruktijden heeft. De 10 snelste brandweerkorpsen in Denemarken zijn brandweerkorpsen van dit bedrijf. Daarnaast is Denemarken een van de goedkoopste landen in de wereld als het gaat om de kosten voor brandbestrijding, zo blijkt uit cijfers van de World Fire Statistics, die de Geneva Association publiceert. De Geneva Association verklaart de lage kosten van de brandbestrijding in Denemarken als volgt: ‘De lage kosten in Denemarken kunnen worden verklaard als gevolg van branddiensten door het particuliere bedrijf Falck, dat in 2011 ongeveer 65% van de Deense gemeenten werkzaam is en zich ook internationaal uitbreidt. De kosten van het bedrijf worden laag gehouden door onder andere een combinatie van brandweer-, ambulance- en wegenwachtdiensten, vanuit hetzelfde gebouw te leveren’.

Burgemeester Ole Bjørstorp noemt goede communicatie, snelle en flexibele oplossingen bij problemen en het gebruik van Falck’s nationale en internationale ervaring als voordelen van de samenwerking. Maar welke invloed heeft de keuze van een private leverancier op de uitvoering van de brandpreventie? “Kijkend naar de brandpreventie, ervaar ik dat er nu meer tijd voor en meer focus op dit werk aanwezig is. Dit komt omdat onze eigen preventieofficieren zich geen zorgen meer hoeven te maken over de aansturing van de brandweerlieden en dus veel meer tijd hebben om zich te concentreren op de brandpreventie. Ook op het gebied van de sociale veiligheid is er een goede en vruchtbare samenwerking tussen gemeenten en het bedrijf. Zo, zijn er in sommige gemeenten jeugdbrandweren opgericht met moeilijk hanteerbare jongeren. Dit heeft al tot positieve resultaten geleid in de vorm van een lagere criminaliteit”, zegt de burgemeester.

Wat betekent een private leverancier van brandweerzorg voor de van ouds nauwe relatie tussen de burgemeester en de brandweerlieden? “Het eerlijke antwoord is dat de afstand wel groter is geworden, omdat de eerste managementlaag binnen de hiërarchie, die van het betreffende bedrijf is. Maar dat beschouw ik juist als een voordeel. Het is beter zo, want zo kan het gemeente bestuur en de gemeentelijke politiek meer onafhankelijk haar beslissingen nemen. Maar uiteraard zijn er genoeg gelegenheden om een goede relatie met de brandweerlieden te onderhouden, ik ben en blijf tenslotte de baas van de brandweer”, concludeert burgemeester Ole Bjørstorp met een glimlach.

Ira Helsloot,
hoogleraar Radboud Universiteit Nijmegen/Crisislab
Astrid Scholtens,
Crisislab

Hoe overleef ik een crisis?

De ondertitel 'Hoe word je zelfredzaam bij rampen?' van het boekje 'Hoe overleef ik een crisis' van auteur Dick Berts beloofd veel goeds. Met zijn boekje wil de auteur de lezer bewust maken van de noodzaak om tijdens crises zelfredzaam te zijn. Bezien vanuit de eigen verantwoordelijkheid die burgers ook bij crises hebben en het feit dat burgers in de eerste uren van een crisis op zichzelf zijn aangewezen, juichen wij als pleitbezorgers van een realistische omgang met 'zelfredzaamheid' een dergelijk initiatief natuurlijk van harte toe.

Maar het eerste deel van het boekje maakt duidelijk dat de motivatie van de auteur om burgers zelfredzaam te laten zijn, voortkomt uit allerhande complottheorieën. Volgens de auteur zijn wij tijdens een crisis volledig op onszelf aangewezen, omdat Nederland een falende en 'liegende overheid' kent die vooral uit 'doofpotburgemeesters' bestaat. Zo wordt het bewust 'falen' van www.crisis.nl tijdens de Moerdijkbrand door de auteur zelfs vergeleken met een-zelfde bewuste overheidsactie als Mubaraks stilleggen van het internet tijdens de volks-opstand in Egypte.

We weten echter dat burgers afhankelijk zijn van feitelijke informatie over (de effecten van) een crisis om werkelijk effectief zelfred-zaam te kunnen zijn. Informatie over de 'big picture' zal grotendeels van de overheid moeten komen. Het helpt dus niet om het vertrouwen van burgers in de overheid te ondermijnen. We weten ook dat burgers zich alleen voorbereiden op rampen die zij als reëel beschouwen. De rampen in het boek zijn worst case gevallen zoals ergst denkbare overstromingen die de hele Randstad verzwelgen, die ver van ieders inlevingsvermogen staan. Daar gaat geen burger zich op voorbereiden. Dus alleen al door zijn aanvliegroute gaat de auteur niet bereiken wat hij naar eigen zeggen beoogt.

Het tweede deel dat werkelijk ingaat op het overleven van rampen is overigens aardig om te lezen. Zonder 'Katadyn waterfilter' houd je het niet lang uit, dat wordt de lezer wel duidelijk gemaakt. De lijsten achterin het boekje voegen echter weinig toe aan de bekende 'denk vooruit' check lijstjes. Jammer trouwens dat de lijstjes niet gekopieerd mogen worden om als checklist-jes in de trapkast te hangen: 'Niets uit deze uitgave mag worden verveelvoudigd …' stelt het colofon nadrukkelijk. Een punt dat ons in lijstjesverband bezighoudt, is dat in dit boekje (net zoals in het Rijksnoodpakket) het fluitje op de lijst van essentiële zaken staat om 'verdwaalde familieleden te vinden en om hulp te kunnen roepen'. Bij een ergst denkbare overstroming?

Een fundamenteel probleem is ons inziens dat het boek inconsistent is: de wereld staat op het punt te vergaan maar de crisisover-leeftips zijn gericht op het overleven van een korte periode voordat de nutsvoorzie-ningen etc. weer draaien. Zo erg is het dus blijkbaar ook weer niet gesteld met onze maatschappij en onze overheid.

Dus samenvattend:

- Uitgaan van – wat ons betreft – absurde complottheorieën gaat mensen niet helpen al was het alleen maar omdat mensen informatie van de overheid nodig hebben om (zelf)redzaam te kunnen zijn.
- Uitgaan van het worst case scenario dat de wereld vergaat, sluit niet aan bij de zelfredzaamheidtips die de auteur geeft.

Wie hoopt op een boekje in de traditie van de urban survival waarvan in Nederland Christo Motz een bekende deskundige voorganger is, komt dus feitelijk bedrogen uit.

D. Berts, *Hoe overleef ik een crisis? Hoe word ik zelfredzaam bij rampen?*, Breda: Papieren Tijger, 2011. ISBN 9789067282628

Katinka van der Hooft,
projectleider zelfredzaamheid
Maaike van Tuyll,
oud-projectleider zelfredzaamheid, plv. programmamanager Dreigingen en Capaciteiten directie Nationale Veiligheid, Nationaal Coördinator Terrorismebestrijding en Veiligheid

Zelfredzaamheid in **noodsituaties**

De afgelopen jaren heeft bij het ministerie van Veiligheid en Justitie het project Zelfredzaamheid bij rampen en crises gelopen. Een project waar veel mensen vanuit de praktijk bij betrokken zijn geweest. Het project loopt ten einde, een goed moment om de geleerde lessen – zonder dat we pretenderen volledig te zijn – uit te dragen.

Belangrijk voor het project is de expertgroep zelfredzaamheid geweest onder leiding van de heer Jan Mans. De expertgroep heeft gedurende het project gezorgd voor onafhankelijk advies bij onder meer een aantal pilots en onderzoeken. Verder heeft zij een belangrijke bijdrage geleverd bij het onder de aandacht brengen van het belang van zelfredzaamheid.

Mensen willen zelfredzaam zijn....
In de praktijk blijkt dat de neiging om zelfredzaam te handelen een gegeven is. Mensen willen zichzelf kunnen redden. Zelfredzaamheid grijpt terug op het basale overlevingsinstinct en is daarmee niet alleen een middel, maar voor individuen ook een doel op zich.

.... maar weten niet altijd hoe het best te handelen
De uitkomst en kwaliteit van het zelfredzame handelen staan echter niet vast en zijn tot op zekere hoogte beïnvloedbaar. Op welke wijze deze beïnvloeding kan plaatsvinden, was de centrale vraag van het project.

Welke lessen zijn er geleerd?
In de afgelopen jaren is voor het vergroten van de zelfredzaamheid zowel op landelijk als op regionaal niveau vooral ingezet op het stimuleren van individuele voorbereiding door burgers op noodsituaties. Het ging dan om voorbereiding in de vorm van kennis (van risico's en van handelingsperspectieven), kunde (aanleren van vaardigheden) en materieel ('noodpakket').

Uit de ervaringen die zijn opgedaan in het project blijkt dat dit onvoldoende is, wil (zelf)redzaamheid werkelijk een bijdrage kunnen leveren aan het verkleinen van de impact van noodsituaties. De rol van bedrijven, hulpverleningsdiensten en individuele hulpverleners is eveneens van essentieel belang, in de voorbereiding op maar ook tijdens een crisissituatie.

Hieronder volgt een impressie van de geleerde lessen.

Les 1 – Stimuleren van voorbereiding op noodsituaties blijft belangrijk, maar moet wel relevant zijn en dicht bij huis
Voor de meeste mensen is het voorbereiden op een grotere of kleinere noodsituatie geen vanzelfsprekendheid. De overheid heeft een aantal jaren via Postbus 51 campagnes ('Denk Vooruit' en 'Goed voorbereid zijn, heb je zelf in de hand') burgers gestimuleerd om zich voor te bereiden.

Deze landelijke campagnes, gericht op het algemeen publiek, helpen vooral bij het vergroten van de intentie om zich voor te bereiden, en bij het creëren van draagvlak voor het onderwerp. Het feitelijk treffen van voorbereidingen wordt eerder gestimuleerd door op regionaal en lokaal niveau activiteiten op te zetten: op maat en herkenbaar voor de persoonlijke situatie. Bij lokale campagnes liggen kansen. Een aantal regio's heeft hier al ervaring mee opgedaan.

Les 2 – Bedrijven zijn een belangrijke schakel om burgers te bereiken (zeker wanneer zij kwetsbare personen of kwetsbare processen herbergen)
De ervaring leert dat de overheid in de eerste plaats een stimulerende rol heeft om de bedrijven/ondernemers en hun gasten bewust te maken van hun eigen mogelijkheden en verantwoordelijkheid. Belangrijk is dat beide groepen de urgentie van de noodsituatie onderschrijven. Vervolgens is het de kunst voor overheden om ook weer een stap terug te doen en niet teveel te gaan voorschrijven.

Les 3 – Adequate crisiscommunicatie helpt mensen om zelfredzaam te kunnen handelen
Voorbereiding is belangrijk maar het is onmogelijk om op alles volledig voorbereid te zijn. Er zijn ook factoren tijdens een noodsituatie die kunnen bijdragen aan zelfredzaam handelen. Eén van die factoren is crisiscommunicatie. Door de opkomst van de sociale media wordt de uitdaging voor de overheid steeds groter om snel, open en duidelijk te communiceren. Het is meestal geen optie meer om te wachten met communi-

ceren totdat er meer helderheid is over de situatie. Op dat moment is het 'geruchtencircuit' al in volle gang. In professionele organisaties beschikken medewerkers op het gebied van crisiscommunicatie onder meer over een mandaat om te bevestigen wat zichtbaar is voor het publiek en te vertellen wat de overheid in het werk stelt om de crisis te bestrijden. Ook kan er aandacht uit gaan naar het aandragen van concrete handelingsperspectieven.

Bijvoorbeeld: er is een winterse stroomstoring. Bij hulpdiensten gaat de aandacht in de meeste gevallen eerst uit naar het patrouilleren en het lokaliseren en helpen van verminderde zelfredzamen. De zelfredzamen worden verondersteld zich zelf te kunnen redden. Echter ook deze groep kan risico's lopen (gebruik gaskachels en ramen dicht – koolmonoxidevergiftiging – gebruik kaarsen – brand). Door direct aan het begin van de stroomstoring enkele concrete handelingsperspectieven te communiceren, help je deze groep de storing goed door te komen en kan vervolgens de aandacht uitgaan naar de groepen die meer hulp nodig hebben.

Goed om nog te noemen is ook dat het rijk samen met de veiligheidsregio's bezig is met de invoering van NL Alert. Hiermee kunnen burgers bij rampen of crises snel worden gewaarschuwd en handelingsperspectief worden geboden.

Les 4 – Hulpverleners moeten in een noodsituatie zelfredzaamheid optimaal benutten en onderdeel maken van hun processen
Naar aanleiding van onderzoek is de aanbeveling om burgers te laten helpen als dat veilig kan en alleen voor die taken die ze aankunnen. Bijvoorbeeld bijdragen aan het waarschuwen van de bevolking, afzetten en afschermen, voorzien in primaire levensbehoeften of het registeren van slachtoffers. Daarbij helpt het om duidelijke instructies en feedback te geven en regelmatig te controleren of de hulpverlening nog goed verloopt. Het is ook van belang om burgers zowel tijdens het incident als achteraf erkenning te geven voor hun inzet.

Les 5 – Om zelfredzaamheid in de warme fase optimaal te kunnen benutten, moeten hulpverleningsdiensten zich hier in de koude fase op voorbereiden
De afweging hoe (zelf)redzaamheid optimaal benut kan worden, moet tijdens ieder incident opnieuw worden gemaakt. Deze afweging kan echter niet goed plaatsvinden als er in de 'koude fase' niet is nagedacht op welke wijze zelfredzaamheid onderdeel uit kan maken van hulpverleningsprocessen en hoe zij deze kan versterken.

Als hulpdiensten zelfredzaamheid optimaal willen benutten moet het in de hele organisatie en in alle fasen van de crisisbeheersing en rampenbestrijding gedragen worden. Dus, integraal onderdeel uitmaken van beleid en operationeel handelen en wel zo dat het aansluit bij bestaande werkwijzen. Het is ook goed om al in de voorbereidende fase beter rekening te houden met burgerparticipatie door het op te nemen in opleidingen van hulpverleners, door burgers te betrekken bij oefeningen en door het (procesmatig) op te nemen in planvorming.

Hoe verder?

Belangrijk is dat de regio's verder gaan met de geleerde lessen. Hier is in veel opzichten veel winst te behalen. Zelfredzaamheid is een gegeven. De kwaliteit van de uitkomsten van dit handelen is echter te beïnvloeden!

Een goede zaak is dat er al meerdere regio's actief aan de slag zijn met zelfredzaamheid. Er is ook al het initiatief genomen om het thema op te nemen in de brandweeropleiding. De experts uit de (voormalige) expertgroep hebben te kennen geven het onderwerp waar mogelijk te willen blijven ondersteunen. Onderling kan men ook nog veel leren van elkaars ervaringen en expertise op dit vlak. Om dit ook op een makkelijke manier mogelijk te maken wordt er door de partners NIFV, TNO, Crisislab, Arq/Impact, 2BSafe en HKV momenteel gewerkt aan het oprichten van een kennis- en expertisecentrum, dat medio dit jaar van start gaat. Voorafgaand aan de oprichting van dit kenniscentrum worden de regio's actief benaderd om mee te denken over de inrichting van dit centrum en om reeds beschikbare kennis uit te wisselen.

dr. José Kerstholt,
senior onderzoeker beslisgedrag, TNO
dr. Marcel van Berlo,
teamleider Community Resilience, TNO

Wereldwijd is er een toename van natuurrampen zoals aardbevingen, orkanen, tsunami's en overstromingen. Alleen al vorig jaar hadden we te maken met een grote overstroming in Australië, de aardbeving in Nieuw Zeeland, de tsunami in Japan en vele andere natuurrampen met groot menselijk, ecologisch en economisch leed. Verwacht wordt dat dergelijke natuurrampen alleen maar zullen toenemen waardoor ook de druk stijgt hoe we de negatieve gevolgen van dergelijke rampen zoveel mogelijk kunnen beperken. Los van het feit dat de capaciteit van professionele hulpdiensten bij dergelijke grootschalige rampen eigenlijk per definitie ontoereikend is, tonen casestudies duidelijk aan dat burgers een belangrijke rol hebben in crisismanagement[1]. Burgers zijn ter plekke, zijn bereid om te doen wat nodig is en hebben kennis van de lokale situatie.

Community resilience: de **ontbrekende schakel** tussen zelfredzaamheid en crisisbeheersing

en in planvorming. De Nederlandse overheid heeft zich tot dusverre vooral op de zelfredzaamheid van het individu gericht: hoe worden burgers zich bewust van de risico's die hen bedreigen in hun lokale omgeving en hoe kunnen ze zich op mogelijke calamiteiten voorbereiden? Maar gaat het bij rampen wel om individuele acties? Of opereren mensen vooral vanuit een sociaal netwerk (de community) waartoe zij op dat moment behoren? Zou het versterken van de veerkracht van communities niet veel meer rendement opleveren? En hoe kan dat dan worden aangepakt?

Community resilience

Communities zijn er in alle soorten en maten: een geografisch afgebakende gemeenschap, zoals een buurt of een wijk, maar bijvoorbeeld ook een groep mensen met gemeenschappelijke interesses en overtuigingen (bijvoorbeeld een geloofsgemeenschap) of een ad hoc community die zich manifesteert via sociale media. Iedereen maakt deel uit van één of meerdere communities.

Bij calamiteiten zal de community waartoe men op dat moment behoort een belangrijke invloed hebben op het gedrag van mensen. Weet men elkaar te vinden? Staan er natuurlijke leiders op? Welke communicatiekanalen heeft men ter beschikking? Dergelijke kenmerken van communities bepalen te zamen hoe veerkrachtig of 'resilient' de community is, dat wil zeggen in hoeverre de community zich kan herstellen van een tegenslag.
Om de veerkracht van een community te versterken zou op verschillende capaciteiten ingezet kunnen worden. Het gaat er daarbij dus niet om de veerkracht in één specifiek domein te versterken, maar het onderliggende idee is dat veerkrachtige communities in staat zijn om een breed scala van tegenslagen op te vangen; niet alleen natuurrampen, maar ook issues op het gebied van de sociale veiligheid of de zorg. Het versterken van de veerkracht van communities is dus maatwerk, afgestemd op de behoeften van die specifieke community ('one size does not fit all').

[1] Bijvoorbeeld K. Groenewegen-ter Morsche en N. Oberijé, *Burgers bij de bestrijding van rampen: betrokken, beschikbaar, bekwaam. Een onderzoek naar praktijkervaringen met burgerparticipatie bij 10 rampen en incidenten in Nederland*, Arnhem: NIFV 2010.

'Whole Community Approach'

De Amerikaanse Federal Emergency Management Agency (FEMA) hanteert voor het versterken van de veerkracht van communities de 'Whole Community Approach'. Kortweg komt deze benadering er op neer dat alle relevante stakeholders (burgers, overheid, bedrijven, NGO's etc.) gezamenlijk inventariseren wat de behoeftes zijn van een community en bepalen wat er nodig is om activa, capaciteiten en belangen te organiseren en te versterken[2].

Er zijn drie centrale principes die aan de *Whole Community* benadering ten grondslag liggen: 1) Begrijp en kom tegemoet aan de feitelijke behoefte van een community; 2) Betrek en 'empower' alle stakeholders in een community en 3) Versterk wat op dagelijkse basis al goed werkt in een community. Het initiatief ligt dus in belangrijke mate op lokaal niveau.

Gezamenlijke inspanning

Burgers hebben een veel centralere rol (gekregen) bij de bestrijding van crises, niet alleen omdat zij ter plekke zijn en (deskundige) hulp kunnen bieden, maar ook omdat zij via sociale media snel een groot publiek kunnen bereiken. Bijvoorbeeld, binnen twee uur nadat het popconcert 'Pukkelpop' was geteisterd door een storm, had een omwonende al het initiatief #Hasselthelpt opgestart. Door dit initiatief werd enorm veel hulp aangeboden zoals slaapplaatsen, voedsel, transport en internet. Een ander voorbeeld is de zogenoemde *Mud Army* die in de Australische stad Brisbane werd gemobiliseerd op initiatief van en gefaciliteerd door de gemeente. Duizenden burgers meldden zich aan om alle modder na de overstromingen op te ruimen. Dit laat zien hoe een dergelijke ad hoc community in staat is om in korte tijd hulp van velerlei aard te organiseren en toont aan hoe sociale media de veerkracht van communities kunnen bevorderen.

Voor het versterken van de veerkracht van communities en het vormgeven van de interactie tussen overheid en burgers kunnen we leren van het buitenland, waar men veel meer ervaring heeft met de voorbereiding op, bestrijding van en herstel na (grootschalige) rampen. Om de informatie-uitwisseling tussen landen te bevorderen heeft het *Department of Homeland Security* (DHS, VS) in 2009 het initiatief genomen om een werkgroep in te stellen waar verschillende landen in vertegenwoordigd zijn. In 2009 is begonnen met zes landen (VS, Australië, Canada, Verenigd Koninkrijk, Zweden en Nederland) wat inmiddels is uitgebreid met Singapore, Duitsland en Nieuw Zeeland.

Een faciliterende overheid

Veiligheid is niet slechts een onderwerp voor beleidsmakers, maar houdt ook burgers bezig: een veilige straat waar kinderen kunnen spelen, een veilige buurt waar je 's nachts over straat kunt gaan, een veilig huis waar de kans op inbraak en brand minimaal is en een veerkrachtige omgeving die adaptief reageert op een pandemie of gifwolk. Voor burgers maakt het daarbij niet uit of het om fysieke veiligheid of sociale veiligheid gaat of dat het de verantwoordelijkheid is van de brandweer of van de gemeente. Het gaat om de veiligheid, of breder nog, het welzijn van hún buurt.

De community zou daarom het uitgangspunt moeten zijn voor interventies die veerkracht moeten versterken: niet het domein of de kolom is bepalend, maar de behoeftes van de community. In het dagelijks leven zijn communities doorgaans al zeer bedreven in het benutten van mogelijkheden. Denk aan het regelen van activiteiten rond het onderhouden van beplanting in de buurt of het werven van vrijwilligers voor de voedselbank. Voor de (lokale) overheid bieden bestaande structuren een uitgelezen kans om ze te ondersteunen en daarmee te versterken. Veel valt daarbij te leren van de interventies op het gebied van sociale veiligheid die al op dit community niveau inspelen. Binnen dit domein wordt zelfs al gesproken van een participerende politie in plaats van participerende burgers. Een faciliterende overheid, gericht op het versterken van de sociale infrastructuur, bevordert de weerbaarheid en veerkracht van communities, en uiteindelijk dus ook van de samenleving als geheel. Community Resilience is de ontbrekende schakel tussen zelfredzaamheid en crisisbeheersing.

[2] FEMA, *A whole community approach to emergency management: principles, themes and pathways for action*. FDOC 104-008-1/ December 2011.

Désirée Geerts,
werkzaam bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid

Security Awareness & Performance (SA&P)

Na de inbraak in een bedrijf gaf iemand aan: Ja, ik vond het al vreemd dat daar iemand liep. Nadat twee mannen zijn opgepakt, omdat ze beveiligingscamera's fotografeerden, bleken diverse mensen ze al gezien te hebben. Na een demonstratie van een actiegroep herinnert een medewerker zich dat een paar weken daarvoor iemand wel heel geïnteresseerd was in zijn werk en opvallend veel wilde weten.
Vaak blijkt na een incident dat mensen iets hebben gezien waarvan ze zich afvroegen: Hé, klopt dat wel? In voorgaande situaties zijn de gevolgen nog beperkt. Het kan ook gaan om een aanslag met een enorme impact. De potentiële schade van zo'n aanslag voor mensenlevens, infrastructuur en maatschappelijke ontwrichting is nog altijd zeer groot.

Waarom aandacht voor security awareness?

Alerte, veiligheidsbewuste medewerkers kunnen in hun eigen werkomgeving vaak als eerste afwijkend gedrag of een afwijkende situatie signaleren en zijn daarom onmisbaar om (de voorbereiding van) mogelijk terroristische activiteiten in de kiem te smoren. En veiligheidsbewustzijn levert nog meer op. Het helpt ook bij het voorkomen van criminaliteit, spionage, vandalisme en acties van extremisten.
Er wordt vaak veel geïnvesteerd in fysieke beveiligingsmaatregelen (*safety*), zoals toegangspasjes, camera's en sloten. Als medewerkers hiermee niet juist omgaan, is een organisatie alsnog onvoldoende beschermd tegen mensen die kwaad willen. Veiligheidsbewustzijn is daarmee een belangrijke voorwaarde voor de veiligheid van de medewerkers en voor de nationale veiligheid in het algemeen.
Daarnaast heeft een organisatie er op diverse manieren baat bij. Security awareness voorkomt verstoring van bedrijfsprocessen, bespaart geld, is in het belang van de bedrijfscontinuïteit, helpt imagoschade te voorkomen en draagt bij aan klantvriendelijkheid en serviceverlening. Onderzoek op bijvoorbeeld het gebied van beveiliging van de burgerluchtvaart heeft uitgewezen dat aandacht voor security binnen een organisatie pas effectief is, wanneer het een continu proces betreft. Daarom is gekozen voor een programmatische aanpak met een publiekprivaat karakter. Aangezien circa 75 % van de vitale infrastructuur in handen is van private bedrijven, is een nauwe samenwerking tussen overheid en bedrijfsleven van cruciaal belang.

Wat houdt het programma in?

In het programma Security Awareness & Performance (SA&P) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid staan het veiligheidsbewustzijn (security awareness) van medewerkers en het prestatievermogen (performance) van de mens centraal. Het programma is een aanvulling op de reguliere beveiligings- en veiligheidsmaatregelen (safety and security). Het meerjarenprogramma is in 2010 gestart en mede dankzij de inzet van diverse publieke en private partijen zijn er inmiddels flink wat resultaten geboekt. Zo zijn e-learning modules ontwikkeld, is een drietal succesvolle diner pensants voor het topmanagement georganiseerd en zijn de nodige red teaming oefeningen uitgevoerd.

Voor wie is het programma bestemd?

Het programma geeft deze kennis en instrumenten aan bedrijven die een vitale functie hebben voor de Nederlandse samenleving, bijvoorbeeld in de energie-, ICT/Telecom-, transport- en financiële sector. Ook chemische, biologische, radiologische en nucleaire (onderzoeks)instellingen zoals ziekenhuizen, laboratoria en universiteiten behoren tot de doelgroep. Binnen het SA&P programma is niet alleen aandacht voor security professionals en medewerkers op de werkvloer, maar ook voor het (top)management.

Welke instrumenten zijn beschikbaar?

Quick scan 'Security Awareness in uw organisatie'
Met behulp van deze quick scan kan snel een eerste indruk worden verkregen van de mate waarin security awareness bij de medewerkers in een organisatie is

ontwikkeld. Heeft een organisatie een security awareness programma en voldoet dat? En is zo'n programma er nog niet, loopt de organisatie dan geen onnodig risico? De quick scan laat zien waar verbetering mogelijk is.

E-learning module Zeker van je Zaak

Medewerkers leren in deze basismodule scherper te kijken naar mogelijke risico's en bedreigingen in hun eigen werkomgeving, wat zij daarvan kunnen merken en wat zij daar zelf aan kunnen doen. Het workshop-materiaal is in het Engels verkrijgbaar onder de naam *It's your business to be sure*.
Naar aanleiding van *Zeker van je Zaak* is een effectmeting uitgevoerd. Uit deze nulmeting blijkt onder meer dat medewerkers zich niet vaak betrokken voelen bij security awareness en dat veiligheidsprofessionals onvoldoende voorlichtingsmateriaal tot hun beschikking hebben. Uit de effectmeting na gebruik van Zeker van je Zaak blijkt dat nut en noodzaak van security awareness door medewerkers meer wordt erkend en dat medewerkers zich meer betrokken voelen bij het onderwerp.

E-learning module dierenrechtenextremisme en spionage

De e-learning module Zeker van je zaak is inmiddels uitgebreid met voorbeelden die betrekking hebben op werkwijzen van dierenrechtenextremisten. Tevens is een e-learning module voor de Kwetsbaarheidsanalyse Spionage (KWAS) ontwikkeld.

Serious gaming

Serious gaming ofwel een virtuele oefenomgeving is een geschikt vervolginstrument op de e-learning-modules. De serious game zorgt voor bewustwording, voor het verkennen van nieuwe situaties en voor het uitproberen van nieuw gedrag. De game biedt medewerkers de gelegenheid om op een veilige manier kennis te maken met potentieel onveilige situaties. Momenteel is een serious game security awareness in ontwikkeling. De NCTV werkt hierbij nauw samen met domeinexperts en stakeholders.

Red teaming

Deze onaangekondigde fysieke- en cyberoefeningen worden jaarlijks in opdracht van het topmanagement van het bedrijfsleven bij een aantal eigen objecten uitgevoerd. Door middel van deze oefeningen wordt inzicht verkregen in (nieuwe) kwetsbaarheden en in de te treffen veiligheidsmaatregelen. Door het koppelen van de expertise van diverse partijen wordt het realistische karakter versterkt. De confidentiële resultaten worden ter beschikking gesteld aan het betrokken topmanagement, zodat deze inzicht verkrijgt in de resultaten en zelf ter verbetering maatregelen kan treffen. Tevens worden de eventuele kwetsbaarheden en beperkingen vertrouwelijk gedeeld,met de doelgroep waardoor de lessen uit een oefening een groot bereik krijgen.

CEO diner

Jaarlijks wordt voor het topmanagement van het bedrijfsleven een diner pensant georganiseerd. Waar safety-aspecten al een plaats hebben op de strategische agenda van organisaties, zou security awareness dat ook moeten krijgen. Najaar 2011 werd speciale aandacht besteed aan de cyber security strategie en de lessen van DigiNotar.

Tot slot

Naast het CEO diner, red teaming en serious gaming krijgen in 2012 ook security awareness bij social media en security awareness bij werving, selectie en uitdienst-treding de nodige aandacht. Dit laatste gebeurt in samenwerking met de Dienst Justitiële uitvoerings-dienst Toetsing, Integriteit en Screening (Justis).

De quick scan en de e-learning modules zijn beschikbaar via www.nederlandtegenterrorisme.nl
Voor meer informatie over het SA&P programma kunt u contact opnemen via info@nctv.minvenj.nl.

Jan Bos,
Bureau Communicatie NCTV

Met bijdragen van:
Esther van Beurden en Petra Timmers,
Directie Cyber Security, NCTV

Nationale Cyber Security Strategie stevig in de steigers

Sinds september vorig jaar staat digitale veiligheid hoog op de politieke agenda. Dat werd nog eens extra duidelijk door de electronische inbraak bij DigiNotar, het bedrijf dat de certificaten voor veel overheidssites verzorgt. Door de fraude met beveiligingscertificaten die daarvan het gevolg was kon een veilig internetverkeer niet meer worden gegarandeerd. En de gevolgen daarvan kunnen verstrekkend zijn. Het belang van een veilig internet kan nauwelijks worden overschat, want de samenleving is sterk afhankelijk geworden van digitale communicatie met als risico dat de samenleving kwetsbaar wordt. In oktober debatteerde de Tweede Kamer met de ministers Opstelten en Donner over Diginotar en de wijze waarop de overheid aandacht besteedt aan cyber security. Naar aanleiding van dat debat heeft minister Opstelten de Tweede Kamer eind vorig jaar uitvoerig geïnformeerd over alle lopende initiatieven.

Met de brief doet minister Opstelten alle toezeggingen die hij inzake cyber security aan de Tweede Kamer had gedaan in één keer gestand. In het AO Nationale Veiligheid van juni 2011 was hij de parlementariërs tegemoet gekomen door toe te zeggen dat nog datzelfde jaar een zogenaamd 'Dreigingsbeeld Cyber Security' zou verschijnen. Daarbij stelde de minister ook een inventarisatie van de juridische knelpunten in het vooruitzicht. Tijdens het plenaire debat van oktober kwam daar de toezegging bij om de Kamer te informeren over taken en ambities van het Nationaal Cyber Security Centrum (NCSC). De motie van het Kamerlid Hennis-Plasschaert om over te gaan tot een wettelijke meldplicht van een inbraak in een voor de samenleving vitaal informatiesysteem werd door de Kamer aangenomen. In de Kamerbrief wordt eveneens ingegaan op de haken en ogen die het realiseren van zo'n meldplicht met zich meebrengt. Hierna wordt op elk van deze onderwerpen nader ingegaan.

Dreigingsbeeld Cyber Security

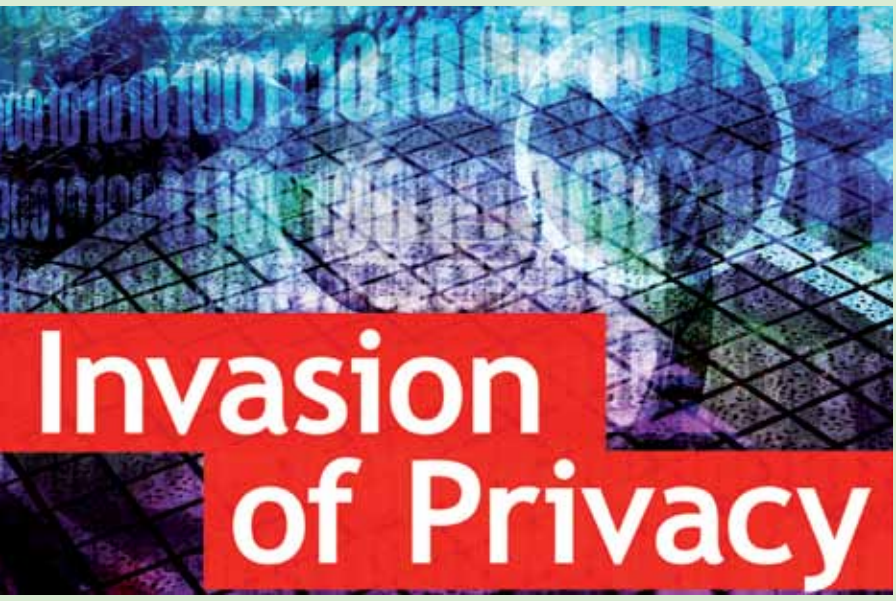
Digitale spionage en digitale criminaliteit zijn de grootste digitale dreigingen waar Nederland nu mee wordt geconfronteerd. In 2011 is een toename van deze incidenten geconstateerd. Zowel overheden als private organisaties zijn regelmatig doelwit van digitale spionage geweest. Deze cyberaanvallen zijn gericht op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde, of op direct geldelijk gewin. Dat staat in het eerste Cybersecuritybeeld Nederland (CSBN) dat minister Opstelten van Veiligheid en Justitie – mede namens zijn collega's van Economische Zaken Landbouw en Innovatie, Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Buitenlandse Zaken - naar de Tweede Kamer heeft gestuurd. Het CSBN vloeit voort uit de Nationale Cyber Security Strategie (NCSS) die eerder vorig jaar door het kabinet is vastgesteld. De Cyber Security Raad onderschrijft het geschetste beeld.

Er is sprake van een breed scala aan groepen die om uiteenlopende motieven gebruik maken van technieken en kwetsbaarheden om cyberaanvallen in Nederland uit te voeren. De grootste potentiële cyberdreigingen gaan uit van statelijke actoren en van criminelen. Criminelen veroorzaken het merendeel van alle cyberincidenten, waardoor deze het meest tastbaar zijn voor de samenleving. Statelijke actoren kunnen echter de kennis en middelen mobiliseren om de meest geavanceerde en grootschalige aanvallen uit te voeren.

De toenemende kans op digitale sabotage is zorgelijk, maar digitale criminaliteit behelst het merendeel van alle cyberincidenten en is het meest voelbaar voor de samenleving. De overheid, het bedrijfsleven maar ook individuele burgers lopen een reëel risico om slachtoffer te worden van digitale criminaliteit. De dreiging is het hoogst waar het gaat om bedrijven en burgers. Deze

hoge en zich snel ontwikkelende dreiging brengt hoge kosten met zich mee en groeit nog steeds. Digitale criminaliteit is voor de dader zeer aantrekkelijk. Met een investering van beperkte middelen is de winstgevendheid groot en de pakkans relatief laag. Hightech cybercriminelen lopen voorop in het verbeteren van aanvalsmethoden om hun aanvallen minder zichtbaar en gerichter te maken. Cybercriminelen zijn goed georganiseerd en hebben specialisaties die zij als dienstverlening aanbieden. Zij voeren hun aanvallen uit in tijdelijke samenwerkingsverbanden die zij op internetfora aangaan.

De problematiek die in het CSBN wordt geschetst sluit goed aan op de aanpak die het kabinet eerder vorig jaar al in de Nationale Cyber Security Strategie heeft geformuleerd. Zo is op het terrein van digitale spionage en sabotage een pakket maatregelen ontwikkeld. Voor bedrijven is er bijvoorbeeld een handleiding Kwetsbaarhedenanalyse beschikbaar gesteld waarmee zij hun digitale weerbaarheid kunnen vergroten. Ook wordt er de komende jaren door het Ministerie van Defensie fors geïnvesteerd in het versterken en ontwikkelen van cybercapaciteiten om ook de militaire dreiging die uitgaat van digitale spionage en sabotage het hoofd te kunnen bieden. Op het terrein van digitale criminaliteit neemt het kabinet gepaste actie door onder meer het team high tech crime te versterken. In het kader van de Onderzoeksagenda Cyber Security wordt door publieke partijen, private partijen en wetenschap onder andere gefocust op nieuwe ontwikkelingen en de risico's die daarmee verbonden zijn. Nederland zoekt daarnaast aansluiting met cyber security centra in verschillende landen om kennis en ervaring uit te wisselen. Ook in het herziene NAVO-cyberbeleid is informatiedeling een belangrijke doelstelling waarvoor Nederland heeft gepleit. Daarnaast investeert Nederland in EU-samenwerking. Het kabinet zet dan ook onverminderd in op de in de NCSS ingezette integrale aanpak.



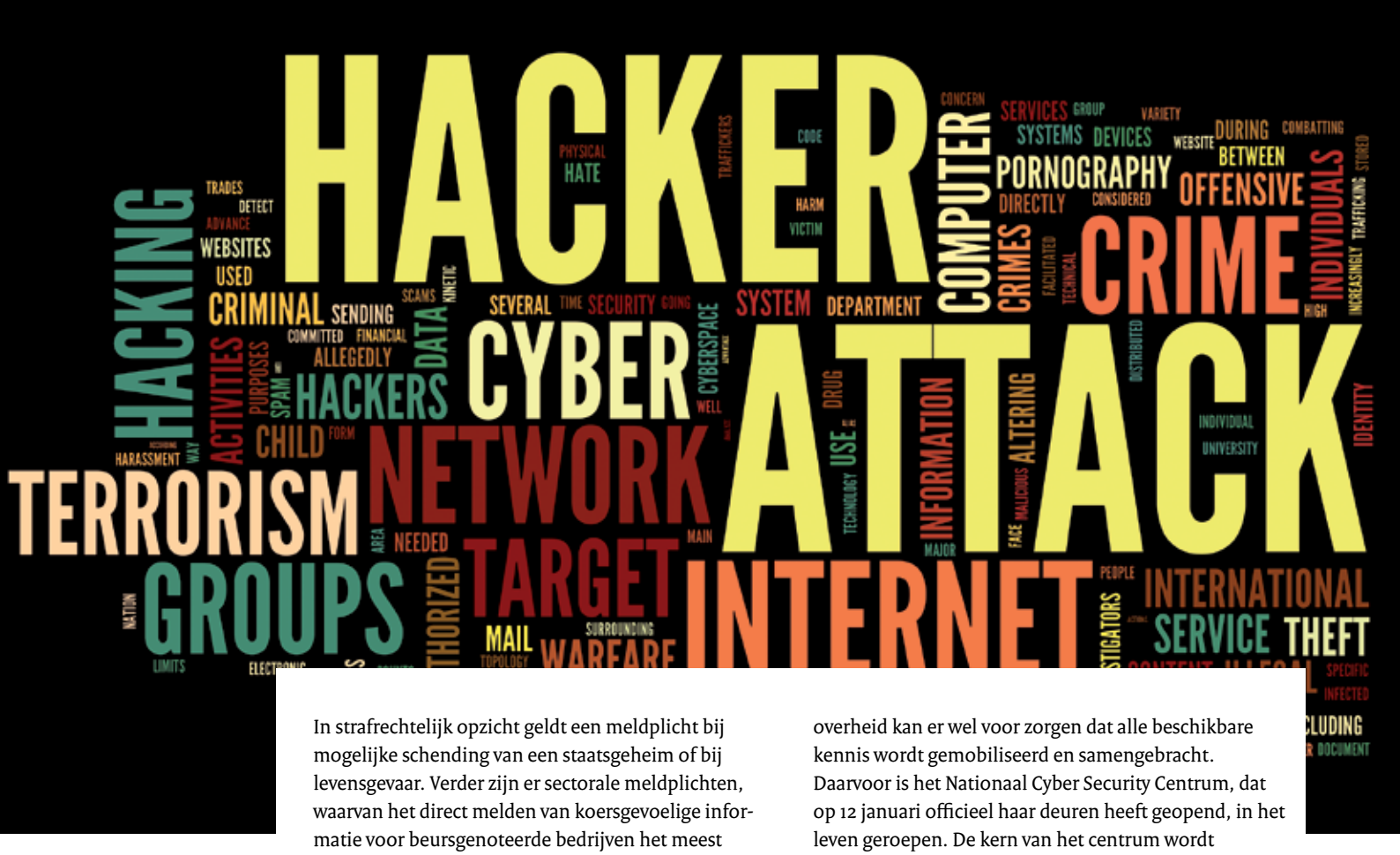
De Cyber Security Raad, die bestaat uit vertegenwoordigers vanuit de top van overheid, bedrijfsleven en wetenschap, onderschrijft het beeld en de daarin genoemde dreigingen. De Raad bepleit dat publieke en private partijen de handen nog meer ineen slaan om het cybersecuritybeeld in de toekomst zowel kwalitatief als kwantitatief te versterken. Ook geeft de Raad de overheid een aantal prioriteiten mee, waarvan het vergroten van ieders bewustzijn voor cyberdreigingen bovenaan staat. Het Kabinet heeft toegezegd de adviezen van de Cyber Security Raad onverkort uit te voeren.

Juridische knelpunten

De wet- en regelgeving die direct of indirect raakt aan de cyber security vormt het juridisch kader waarbinnen uitvoering wordt gegeven aan de Nationale Cyber Security Strategie. De definitie stelt dat onder cyber security moet worden verstaan het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Dat maakt helder dat zowel opzettelijke als onopzettelijke verstoringen tot het werkterrein van de cyber security behoren.

De basis van alle wetgeving, dus ook nieuwe wetten die het bevorderen van de cyber security tot doel hebben, bestaat uit het grondwettelijk en verdragsrechtelijk kader. Daarin is bijvoorbeeld de eerbiediging van ieders persoonlijke levenssfeer vastgelegd. Ook de wettelijke regels over het vastleggen en verstrekken van persoonsgegevens, die de Grondwet voorschrijft, zijn voor cyber security relevant. Daarmee staat de leidraad voor het formuleren van nieuwe wet- en regelgeving vast.

Het bevorderen van cyber security doorloopt verschillende fasen. Het begint met preventie en toezicht, vervolgens is een eventuele meldplicht aan de orde. Daarna kan de overheid besluiten tot interventie, opsporing en repressie, Het juridisch kader gaat op elk van deze vijf fasen specifiek in. De Wet Bescherming Persoonsgegevens – met daaraan gekoppeld het College Bescherming Persoonsgegevens als toezichthouder – is de belangrijkste wet die misbruik moet voorkomen. In aanvulling daarop zijn er regelingen voor verschillende sectoren, zoals de financiële instellingen of de zorginstellingen. In overleg met deze sectoren wordt bekeken of deze regelingen naar aanleiding van moderne ontwikkelingen moeten worden aangepast. Dat geldt ook voor de bevoegdheden waarover de inlichtingen- en veiligheidsdiensten beschikken.



In strafrechtelijk opzicht geldt een meldplicht bij mogelijke schending van een staatsgeheim of bij levensgevaar. Verder zijn er sectorale meldplichten, waarvan het direct melden van koersgevoelige informatie voor beursgenoteerde bedrijven het meest bekend is. Ter bescherming van persoonsgegevens is er voor aanbieders van electronische communicatiediensten momenteel een meldplicht in de maak. En het kabinet heeft aangekondigd met een wet te komen voor een algemene meldplicht in gevallen van verlies, diefstal of misbruik van persoonsgegevens. Het debat over Diginotar heeft geleid tot een nieuw voornemen, namelijk voor een meldplicht van inbreuken voor organisaties betrokken bij voor de samenleving vitale informatiesystemen. Dat is vastgelegd in de motitie van Hennis-Plasschaert die door de Kamer is aangenomen. Deze meldplicht is anders van karakter dan alle andere, omdat hij niet sectoraal is en evenmin alleen betrekking heeft op persoonsgegevens. Dat maakt dat minister Opstelten meer tijd nodig heeft om het wetsvoorstel voor te bereiden. Voor de zomer ontvangt de Tweede Kamer nadere informatie over de inrichting van de meldplicht. Daarbij zal ook worden ingegaan op de mogelijkheden om bij een cybercrisis snel, kundig en niet-vrijblijvend te acteren. Want ook voor dergelijke interventiemogelijkheden is binnen het huidige juridische kader geen direct voor de hand liggende wetgeving aanwezig.

Nationaal Cyber Security Centrum

De Nationale Cyber Security Strategie heeft als titel “Slagkracht door samenwerking” meegekregen. Want cyber security is een dermate veelomvattend en ingewikkeld onderwerp dat samenwerking een absolute vereiste is. De ervaring met de electronische inbraak bij DigiNotar heeft aangetoond dat een crisis het snelst in de kiem kan worden gesmoord wanneer overheid en bedrijfsleven de krachten bundelen. Omdat ICT-systemen overwegend in private handen zijn is de directe invloed van de overheid vaak beperkt. Maar de overheid kan er wel voor zorgen dat alle beschikbare kennis wordt gemobiliseerd en samengebracht. Daarvoor is het Nationaal Cyber Security Centrum, dat op 12 januari officieel haar deuren heeft geopend, in het leven geroepen. De kern van het centrum wordt gevormd door GOVCERT, het team van de overheid dat zich voorheen bezighield met cyber security en respons op incidenten. Anders dan bij GOVCERT is samenwerking tussen publieke en private partijen de basis van het centrum. In eerste instantie zullen de overheidspartijen bij elkaar worden gebracht. En dat zijn er nogal wat. Minstens vijf ministeries zijn bij het onderwerp betrokken: EL&I vanwege de economische importantie, BZK omdat het beheer van de eigen ICT-systemen daar ligt, Defensie gezien de relatie met aanverwante dreigingen als cyberspionage en cyberwarfare en BZ omdat cyber security niet ophoudt bij de landsgrenzen en dus ook onderwerp is van internationale afspraken. Ook de AIVD, het Openbaar Ministerie en het KLPD zijn belangrijke partners. Het ministerie van V&J is vanwege alle aspecten van veiligheid het ministerie dat is belast met de coördinatie.

In 2012 zal worden gewerkt aan aansluiting van steeds meer private partijen en wetenschapsinstellingen. Zo zal het Nationaal Cyber Security Centrum (NCSC) zich langzaam maar zeker moeten ontwikkelen tot hét samenwerkingsplatform en hét expertisecentrum op het gebied van cyber security dat overheden en bedrijven adequaat en bijtijds over mogelijke dreigingen kan adviseren. Mocht het onverhoopt toch nodig zijn, dan komt het NCSC in actie. ‘Rapid response’ is een van de belangrijkste taken. Het incident met DigiNotar heeft aangetoond dat snelheid van handelen cruciaal is om een crisis de kop in te drukken. Zodra daar aanleiding voor is treedt het centrum op tegen dreigingen en incidenten. En mocht een incident desondanks uitmonden in een crisis, dan levert het NCSC alle mogelijke ondersteuning om de crisis zo goed mogelijk te beheersen.

Nationaal Cyber Security Centrum geopend

‘Well done, Netherlands!’

Met een druk op de knop opende minister Opstelten op 12 januari het Nationaal Cyber Security Centrum. Hij zette daarmee een lasershow in werking die door hemzelf als een ‘high tech spektakel’ werd gekenschetst en die het stampvolle World Forum een ludiek beeld gaf van de strijd die het NCSC heeft te voeren met internet-criminelen vanuit de hele wereld. De opening van het centrum had vooral een symbolisch karakter, want het NCSC was al op 1 januari feitelijk van start gegaan. En er is nog veel werk te verzetten voordat het centrum zijn ambitie om uit te groeien tot hét expertisecentrum en samenwerkings-platform op het gebied van cyber security heeft verwezenlijkt. Maar als een goed begin inderdaad het halve werk zou zijn, dan is er op 12 januari al veel bereikt. Samenwerking vormt de basis van het nieuwe centrum, samenwerking binnen de overheid, samenwerking tussen publieke en private partners, samenwerking met de wetenschap en internationale samenwerking. Al die partijen waren op de openings-conferentie ruim vertegenwoordigd. Of het nu was tijdens de plenaire paneldiscussie, in de workshops, op de informatiemarkt, of in de wandelgangen, overal werd in woord en daad uitdrukking gegeven aan de publiek private samenwerking. Minister Opstelten hamerde in zijn openingsspeech op het belang van die samenwerking. ‘Goede samenwerking is in ons aller belang’, aldus de coördinerend minister voor cyber security, ‘samen zijn we in staat ervoor te zorgen dat Nederland – nu en in de toekomst – beschikt over een sterke, veilige en weerbare ICT-infrastrctuur. Zodanig dat hackers, cybercriminelen en andere kwaadwillende geen kans krijgen om cruciale informatie te bemachtigen, onze vitale diensten en systemen aan te vallen, of zelfs plat te leggen.’

Erik Akerboom, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, ging in zijn toespraak nog een stapje verder en maakte het welslagen van het centrum afhankelijk van de samenwerking tussen overheid en bedrijfsleven. ‘Het succes van het NCSC hangt af van de inbreng van informatie en expertise van zowel publieke als private partijen’, luidde zijn stelling. En tegen de partijen die nog aan de zijlijn staan zei hij: ‘we nodigen private en publieke partijen uit om zich in het komende jaar aan te sluiten. Die aansluiting is van groot belang.’ Hij zei dat tegenover een zaal die voor het merendeel bestond uit vertegenwoordigers van private partijen. Voor Wil van Gemert, die op de dag van de opening aantrad als directeur Cyber Security van de NCTV was er op zijn eerste werkdag dus meteen volop werk aan de winkel. Tussen de bedrijven door legde hij contacten met mogelijke samenwerkingspartners en tijdens de paneldiscussie riep hij met name de vitale sector op om binnen het NCSC stevig samen te werken om op die manier de weerbaarheid te vergroten.

Voorafgaand aan de opening door minister Opstelten heette burgemeester Van Aartsen de aanwezigen welkom. Hij toonde zich erg verguld met de aanwezigheid van het NCSC binnen zijn stadsgrenzen. De missie van het nieuwe centrum past naadloos bij het profiel van Den Haag als stad van vrede en veiligheid en draagt tot ver over de landsgrenzen bij aan het imago van de Hofstad. De burgemeester werd op zijn wenken bediend door Eurocommissaris Neelie Kroes die tijdens de openingsplechtigheid – vanaf het videoscherm – het laatste woord had. Als verantwoordelijk commissaris voor de digitale agenda toonde ze zich onder de indruk van de inspanningen die Nederland op het terrein van cyber security verricht. “Well done, Netherlands!” waren dan ook haar afsluitende woorden.

Digitale oorlogvoering
Regels voor geweldgebruik in cyberspace

In elk toekomstig militair conflict zullen digitale middelen een belangrijke rol spelen. De Nederlandse krijgsmacht wil daarom capaciteiten ontwikkelen om in het digitale domein te kunnen opereren. Aan welke internationale regels dient de inzet hiervan te voldoen? De Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) geven hier antwoord op in het advies 'Digitale Oorlogvoering'. Luitenant-generaal b.d. Marcel Urlings, voorzitter van de ingestelde commissie digitale veiligheid, overhandigde het advies medio januari aan de ministers Hillen, Rosenthal en Opstelten. De regering stuurt binnenkort een reactie aan het parlement.

Arjan Uilenreef,
secretaris commissie Digitale Veiligheid,
Adviesraad Internationale Vraagstukken

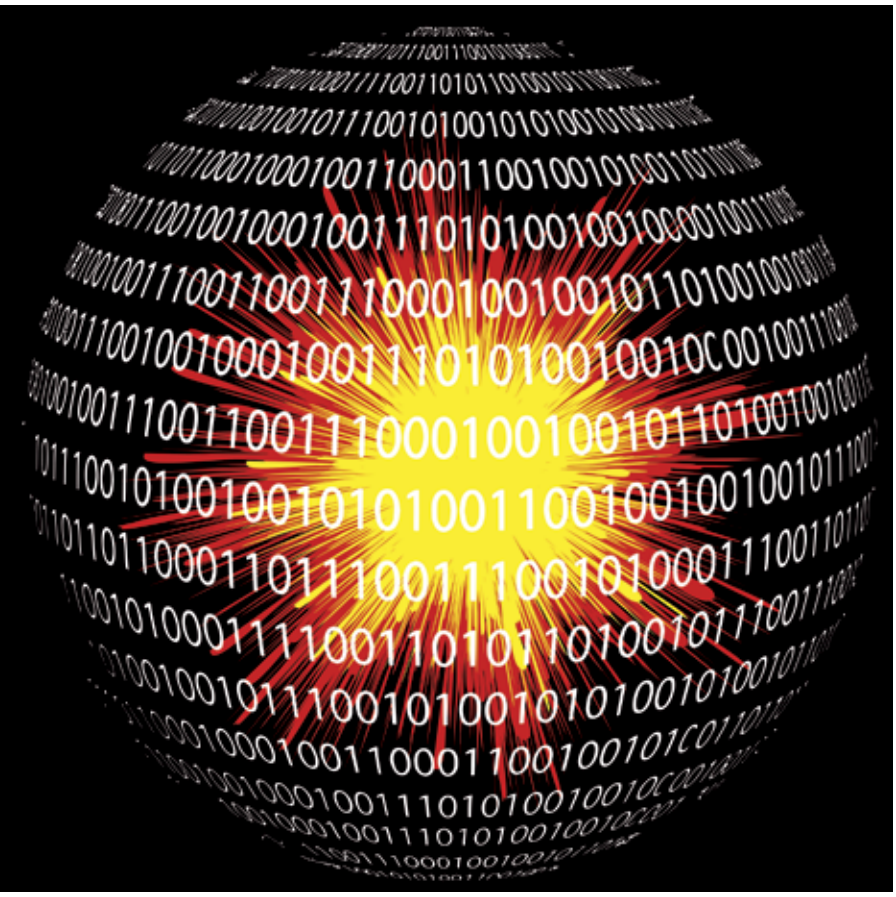
Foto: Maarten Hilbrandie

Doemscenario's

In het publieke debat worden regelmatig doemscenario's geschetst, waarbij de wereld in een soort 'Cyber Armageddon' of een 'Cyber Pearl Harbor' digitaal ten gronde wordt gericht. De opstellers van het advies nemen afstand van dit soort beelden en bepleiten een nuchtere kijk op digitale veiligheid. Een 'cyberoorlog', waarin alleen digitaal heen en weer wordt 'geschoten' en die verwoestende gevolgen kent, is niet aannemelijk. Digitale capaciteiten zullen naar verwachting wel in elk toekomstig conflict een belangrijke rol spelen. Bij een digitale aanval wordt gebruik gemaakt van verschillende technieken, zoals het versturen van kwaadaardige software (*malware*). Hiermee kan bijvoorbeeld een militair communicatie-systeem of de procesbesturing van een fabriek worden beschadigd. Om adequaat te kunnen reageren op digitale dreigingen is een geïntegreerde overheidsbenadering nodig, waarbij zowel militaire als civiele organisaties betrokken zijn. Het rapport stelt met nadruk dat militair ingrijpen pas aan de orde is nadat diplomatieke of strafrechtelijke mogelijkheden zijn benut.

Zelfverdediging

Voor de duidelijkheid: het advies gaat niet in op dagelijkse computeraanvallen zoals die worden uitgevoerd door cybercriminelen. Hiertegen willen overheid en bedrijven uiteraard ook maatregelen nemen. De regering heeft de adviesraden echter expliciet gevraagd zich te buigen over de toepasselijkheid van het recht op zelfverdediging - met het gebruik van geweld - en het oorlogsrecht. Volgens het



advies mag een land zich met geweld verdedigen, dus ook met 'gewone' wapens, wanneer een digitale aanval een aanmerkelijk aantal dodelijke slachtoffers of een grootschalige vernietiging van of schade aan vitale civiele of militaire infrastructuur tot gevolg heeft. Het recht op zelfverdediging is ook toegestaan als een digitale aanval geen fysieke schade tot gevolg heeft, maar er wel sprake is van (een aanhoudende poging tot) ontwrichting van de staat of de samenleving. Het moet dan gaan om meer dan een belemmering bij het normaal uitvoeren van taken. Er wordt benadrukt dat een aanval met deze gevolgen zich tot op heden nog niet heeft voorgedaan. Zelfs de ontregeling van het internetverkeer in Estland in 2007 of de aanval met de Stuxnet-worm op een Iraanse verrijkingscentrale voldeed niet aan de voorwaarden om het recht op zelfverdediging met gewelddadige middelen in te roepen.

Oorlogsrecht

Het gebruik van geweld moet vervolgens wel voldoen aan een aantal voorwaarden. Zo moet er geen redelijk alternatief (noodzakelijkheidsregel) voor een tegenaanval bestaan en mag een land niet overreageren (proportionaliteitsregel). Ook moet er voldoende zekerheid bestaan over de herkomst van de aanval. Betrouwbare inlichtingen zijn daarom vereist voordat een digitale aanval militair kan worden beantwoord. Zodra het een gewapend conflict betreft is het humanitair oorlogsrecht van toepassing. Dit betekent dat er geen burgerdoelen mogen worden aangevallen, zoals het vernietigen van medische systemen in een ziekenhuis of grootschalige verstoring van het elektriciteitsnetwerk. Ook bij digitale oorlogsvoering is het verboden om een neutrale status voor te wenden, bij voorbeeld door IP-adressen van beschermde organisaties als het Rode Kruis te misbruiken. Het advies concludeert kort gezegd dat de bestaande internationale rechtsregels ook op digitale conflicten van toepassing zijn. Een apart cyberverdrag is dan ook niet nodig. Wel is het goed om de deze regels in een internationale gedragscode politiek te onderschrijven. Dit kan de kans op digitale conflicten verminderen.

Innovatieve krijgsmacht

De krijgsmacht moet over digitale kennis en vaardigheden beschikken. Cybercapaciteit hoort thuis in de *toolbox* van een technologisch hoogwaardig Nederlands leger. De opstellers van het advies menen dat bij de ontwikkeling van operationele cybercapaciteit voor de krijgsmacht enige bescheidenheid in acht moet worden genomen. Digitale 'wapens' kennen bij voorbeeld een beperkte houdbaarheidsduur omdat de software waaruit deze feitelijk bestaat snel kan verouderen. Daarnaast vergt het voorbereiden en uitvoeren van een aanval hoogwaardige technische kennis. De schaarse defensiemiddelen zouden daarom vooralsnog slechts op beperkte schaal moeten worden ingezet voor het ontwikkelen van offensieve capaciteiten. De nadruk moet liggen op het verbeteren van de verdediging van de eigen defensienetwerken en het opbouwen van een inlichtingencapaciteit op digitaal gebied.

Cyber Security Centrum

De oprichting van het Nationaal Cyber Security Centrum (NCSC) is een belangrijke ontwikkeling. Juist omdat digitale dreigingen een gezamenlijke overheidsaanpak vergen. Verschillende dreigingsvormen als digitale oorlogvoering, digitale spionage of digitale criminaliteit gebruiken vaak dezelfde technieken. Alleen het beoogde doel verschilt. Het is belangrijk, maar zeker niet eenvoudig, de motieven en identiteit van de aanvaller snel te achterhalen. Mede gezien de schaarse technische kennis en capaciteiten is een ontkokerde aanpak noodzakelijk. Het NCSC kan zich op termijn ontwikkelen tot een soort nationaal *computer emergency response team* (CERT) dat de gezamenlijke monitoring van vitale netwerken voor zijn rekening neemt. Daarbij kan nog meer gebruik worden gemaakt van de capaciteit die aanwezig is bij GOVCERT.NL, MIVD, AIVD, KLPD, soms aangevuld met commerciële en wetenschappelijke organisaties. Op het terrein van inlichtingenverzameling is verdergaande samenwerking tussen de inlichtingenorganisaties AIVD en MIVD mogelijk door *signals intelligence* en cybercapaciteiten in een gezamenlijke eenheid onder te brengen.

Marijke Stokkel,
projectmanager bij het Nationaal Cyber Security Centrum

‘Cyber incidenten **oplossen** kun je niet **alleen’**

Civiel-militaire samenwerking tijdens oefening Cyber Coalition

Na een jarenlang conflict over eigenaarschap van olievelden in de grensregio, valt Kamon begin februari Tytan binnen en bezet diens olierijke gebieden. De VN reageert met economische sancties tegen Kamon en verleent de NAVO het mandaat om via militair ingrijpen Tytan te bevrijden. Daarop onderneemt Kamon meerdere cyberaanvallen: de oliepijplijn systemen van NAVO-landen, waaronder Nederland, worden gecompromitteerd, in diverse media verschijnen verontrustende – achteraf onjuiste – berichten en vertrouwelijke militaire informatie uit NAVO-landen wordt gelekt op sociale media.

Dit fictieve scenario heeft militaire en civiele organisaties van 23 NAVO-landen, waaronder Nederland, drie dagen lang intensief beziggehouden. Dit gebeurde in het kader van de NATO ICT oefening ‘Cyber Coalition 2011’, die van 13 tot en met 15 december 2011 plaatsvond. De Nederlandse deelname is geïnitieerd vanuit DefCERT[1]. Daarnaast waren het Nationaal Cyber Security Centrum (tot eind 2011 Govcert.nl), KPN, Leaseweb en het OM van de partij.

Dit artikel richt zich op samenwerking in de oefening op militair-civiel vlak, in het bijzonder tussen het NCSC en DefCERT. Samenwerking is een essentieel onderdeel van een adequate respons op ICT crises. Dat is ook de mening van Dave Woutersen, security specialist bij NCSC en speler tijdens de oefening. “Samenwerking is de sleutel van ons werk. ICT incidenten oplossen kun je niet alleen, je hebt andere spelers in het werkveld nodig. Je moet elkaar weten te vinden en je hebt onderling vertrouwen nodig.’

De civiel-militaire samenwerking bij Cyber Coalition verliep, na wat opstartproblemen, naar tevredenheid. Tussen het NCSC en DefCERT bestaat de afspraak dat DefCERT zich richt op het behandelen van cyber-incidenten met een specifiek militair karakter en het NCSC de incidenten voor Rijksoverheid (en sinds januari 2012 vitale infrastructuur) voor zijn rekening neemt. Van te voren vroeg men zich af of deze scheidslijn tijdens crises voldoende duide-lijk te maken zou zijn, om te voorkomen dat DefCERT en NCSC zich onbedoeld op elkaars terrein zouden begeven. Tijdens de oefening bleek dit een ongegronde angst; beide partijen hadden een duidelijke focus op hun natuurlijke domein.

Friso Meijer van DefCERT, projectleider Cyber Coalition en ingezet ter ondersteuning van de internationale oefenleiding: “De eerste dag zagen we dat DefCERT en NCSC dezelfde incidenten onderzochten, zonder dit van elkaar te weten. Later ontstond er overleg waardoor de beschikbare expertise en capaciteit van beide teams beter werd ingezet.” De gezamenlijke conference calls waren de start van een gecoördineerde samenwerking. “Vanaf dat moment hebben we elkaar inzicht gegeven in de incidenten waar we mee bezig waren en hebben we werkafspraken gemaakt. Op die manier konden we elkaar helpen bij het oplossen van de incidenten die speelden.” Beide partijen zijn zeer tevreden over deze samenwerking.

Heldere afspraken

Als leerpunt wordt meegenomen hoe de samenwerking tijdens een echte crisis vanaf het eerste begin op effectieve wijze vormgegeven kan worden. Het is goed om hierover vooraf al heldere afspraken te maken. Alle leerpunten van de oefening worden meegenomen in het evaluatietraject, dat momenteel in volle gang is. De NAVO evaluatie richt zich met name op de samenwerking binnen de NAVO en tussen NAVO landen. Daarnaast voeren NCSC en DefCERT hun eigen, interne evaluatie uit. In februari starten de voorbereidingen voor Cyber Coalition 2012. “Met de vorming van het NCSC en de oprichting van het Defensie Cyber Commando gebeurt er bij de overheid veel op het gebied van cyber defense. Tijdens Cyber Coalition 2012 zullen we zien hoe dat het vermogen om te reageren op grootschalige cyberincidenten heeft versterkt.” aldus Friso Meijer.

[1] DefCERT richt zich op de digitale verdediging van de ICT-infrastructuur van Defensie. Daarnaast zal defensie een Defensie Cyber Commando oprichten.

Jorien Holsappel,
Impact, partner in Arq Psychotrauma Expert Groep

Handreiking **Herdenken na een ramp**

Wanneer ergens een schokkende gebeurtenis plaatsvindt, verzamelen zich vaak binnen een paar uur mensen om bloemen, kaarsen en knuffels neer te leggen. Al gauw klinkt de roep om een herdenking. Het plaatst de betrokken overheid voor beslissingen: wie is verantwoordelijk voor het organiseren van een herdenking? Welke vorm moet de herdenking krijgen? Wat is het belang van een herdenking zo kort na de gebeurtenis? Hoe is dat te vertalen in een passend programma?

De afgelopen jaren is hiermee op verschillende plekken ervaring opgedaan. Impact, het landelijk kennis- en adviescentrum voor psychosociale zorg na schokkende gebeurtenissen, heeft ervaringen van organisatoren, geestelijk verzorgers en getroffenen gecombineerd met observaties uit onderzoek, en deze vertaald in een praktische 'Handreiking Herdenken'. De handreiking benoemt aandachtspunten en geeft tips gericht op de keuze of er al dan niet een herdenking moet komen, adviezen voor de inrichting van een projectteam, de opzet van een programma, praktische voorbereidingen en omgang met media-aandacht. Daarbij is oog voor doelen, doelgroepen, belangen en religieuze en culturele diversiteit. Ook wordt aandacht besteed aan de discussie die mogelijk kan ontstaan rond de oprichting en vormgeving een monument.

De handreiking is geschreven in opdracht van het Ministerie van Veiligheid en Justitie en is sinds januari beschikbaar. Alle gemeenten ontvangen kosteloos een exemplaar. Ook is het boekje als pdf te downloaden via: www.impact.arq.org.

1. Denk van tevoren na over doelgroep en doel van de herdenking, zodat iedereen binnen de projectgroep dezelfde uitgangspunten hanteert.
2. Kies voor de herdenking een moment kort na de ramp maar wacht wel tot alle uitvaarten geweest zijn. De herdenking vormt vaak een overgangsmoment van de fase van collectieve rouw naar de fase waarin de samenleving terugkeert naar de gewone patronen.
3. Geef de inhoud van het programma zo veel mogelijk vorm met en vóór de doelgroep. Nabestaanden waarderen het als hen gevraagd wordt mee te denken. Vaak zijn enkele getroffenen bereid om te spreken.
4. Vraag hulp van anderen, zoals de (lokale) Raad van Kerken, een dienst Geestelijke Verzorging, belangenorganisaties van getroffenen van andere rampen, Impact/Arq, ervaringsdeskundigen van andere gemeenten of een uitvaartorganisatie. Je hoeft niet alles te weten, als je contact hebt met wie het wel weet.
5. Voor getroffenen is de ontmoeting met elkaar heel belangrijk. Bied hier de tijd voor in een informeel samenzijn na afloop van het programma.
6. Durf grenzen te stellen aan het programma. Voor het formele gedeelte is de duur van drie kwartier tot een uur een goede richtlijn.
7. Openstaan voor een religieuze dimensie in het programma betekent niet dat de herdenking gevuld wordt met lange gebeden en onbegrijpelijke rituelen; er zijn veel vormen die voor iedereen, ongeacht religieuze achtergrond, een meerwaarde kunnen hebben. Als er wel expliciet aandacht wordt besteed aan de religieuze dimensie, kan dit beperkt blijven tot de religies die onder de getroffenen vertegenwoordigd zijn.
8. Ga zeer zorgvuldig om met het noemen van de namen en het kiezen van symbolen daarbij. Uitspraak en spelling van de namen dienen correct te zijn.
9. Informeer de genodigden van tevoren goed over het verloop van de bijeenkomst en over de afspraken die gemaakt zijn met de pers.
10. Beperk het aantal media dat aanwezig is, maak duidelijke afspraken en zorg voor goede begeleiding.

Bestrijden hoog

Alertheid, daadkracht en goede samenwerking cruciaal

Begin januari 2012 viel in enkele dagen extreem veel regen in combinatie met een aanhoudende noordwester storm. Zowel langs de kust als op het IJsselmeer was er sprake van hoge waterstanden en liep de afvoer van de grote rivieren snel op. Waterschappen hadden moeite met het afvoeren van overtollig water via de sluizen. In de probleemgebieden is met man en macht gewerkt om de situatie onder controle te houden. Naast medewerkers van waterschappen en Rijkswaterstaat die toestroomden uit het hele land werkten ook vrijwilligers soms dag en nacht om de dijken in de kwetsbare gebieden in de gaten te houden. Waterschappen lieten vooraf aangewezen polders vollopen, hebben noodpompen en extra gemalen ingezet, legden tijdelijke nooddijken en evacueerden uit voorzorg de Groningse dorpen Woltersum, Wittewierum en delen van Ten Post en Ten Boer. De berichtgeving in de media stond gedurende enkele dagen volledig in het teken van de wateroverlast.

Hanneke Heeres,
senior communicatieadviseur, Unie van Waterschappen[1]

Landelijk beeld

Waterbeheer in Nederland is in handen van Rijkswaterstaat en de waterschappen. Rijkswaterstaat is verantwoordelijk voor het landelijk watersysteem (de grote rivieren, het IJsselmeer, de Zeeuwse en Hollandse Delta, de zee) en de waterschappen gaan over de regionale watersystemen. Bij problemen met hoog water wordt de Landelijke Coördinatiecommissie Overstromingen (LCO) opgeschaald. De LCO is een onderdeel van het Water Management Centrum Nederland (WMCN) in Lelystad. In dit centrum werkt Rijkswaterstaat samen met het KNMI en de waterschappen om bij extreme omstandigheden op het terrein van waterbeheer juiste en adequate informatie te verschaffen. Dit landelijk waterbeeld wordt samengesteld uit waterbeelden van regionale diensten van RWS en waterschappen en uit actuele informatie en verwachtingen van het KNMI en Rijkswaterstaat.

Overweldigende media-aandacht

Vanwege het samenvallen van springtij en extreem hoge waterstanden in de rivieren en het IJsselmeer is de LCO opgeschaald. Het voortouw van de aanpak van de overlast lag bij de regionale partijen. LCO leverde eenduidige informatie aan over de situatie in het land. Binnen de regio's is samengewerkt tussen waterschappen en veiligheidsregio's. Ook de inzet van het leger is via de regionale kanalen opgepakt. Doordat de media massaal naar het noorden uitrukten, werd de calamiteit in de beeldvorming een landelijk evenement. De

[1] Met medewerking van Michael Bentvelsen (UvW), Ruud van Heel (Waterschap Roer en Overmaas), Gaby Krikke en Sylvia Mosterd (Waterschap Noorderzijlvest) en Claudia Sikes (Waterschap Peel en Maasvallei).

water

snelheid en kwaliteit van de informatievoorziening is van cruciaal belang, zowel bij de interne als de externe communicatie. Gebrekkige informatievoorziening (te laat, onvolledig) blijkt bij evaluaties van calamiteiten het grootste knelpunt. Naast informatie over de organisatie van het waterbeheer heeft de Unie van Waterschappen dagelijks een aantal malen updates over de actuele situatie opgesteld en in- en extern uitgezet.

Er is waar nodig extra mankracht ingezet. Zo hebben communicatieadviseurs van waterschappen waar geen problemen waren het Waterschap Noorderzijlvest tijdelijk versterkt. Ook nu de wind is geluwd, is er nog veel werk aan de winkel. Bewoners in de getroffen gebieden willen weten welke maatregelen er worden genomen om toekomstige calamiteiten te voorkomen. Worden plannen aangepast? Waar en bij wie kunnen zij hun schade verhalen?

Lessen en ervaringen

Een politiek-maatschappelijke discussie over de normen voor dijken is opnieuw op gang gekomen door deze recente ontwikkelingen. Voorzitter Peter Glas van de Unie van Waterschappen: “Uiteindelijk is door grote inzet van zeer gemotiveerde medewerkers en bestuurders voorkomen dat het hoogwater oncontroleerbaar werd. Ik vind dat we hier veel van kunnen leren. Hebben we met elkaar goede afspraken gemaakt over de gewenste veiligheidsniveaus? Hoe zijn taken en verantwoordelijkheden verdeeld? Is onze calamiteitenorganisatie op orde gebleken? En, welke risico’s willen wij accepteren? Het belang van het hebben van voldoende waterbergingen is wederom duidelijk naar voren gekomen. De ruimte voor water (aanvoer, afvoer en berging) is beperkt, want in ons drukbevolkte en bedrijvige land blijft geen meter onbenut. In 1998 liepen we ‘ineens’ tegen de grenzen aan van ons regionale watersysteem, toen in één week tijd in Zuid-Holland de paprika’s in de kassen dreven en in Groningen de aardappeloogst verloren ging. Schade: 400 miljoen gulden.

In het Noorden
Er is in Groningen na de overlast in 1998 stevig ingezet op de samenwerking tussen de gemeenten, hulpverleningsdiensten en waterschappen. Het Groninger model dat hier uit voortkwam heeft mede model gestaan voor de veiligheidsregio's die later in heel Nederland zijn opgestart. In de veiligheidsregio Groningen werken brandweer, politie, GHOR, gemeenten, waterschappen, defensie en de provincie samen. Dat men elkaar goed kent en weet te vinden, op bestuurlijk en ambtelijk niveau, heeft de afgelopen periode zeker vruchten afgeworpen. Daarnaast hebben de waterbergingen die inmiddels zijn gerealiseerd hun nut bewezen.

Waterberging cruciaal

In 2004 zijn tussen het Rijk, waterschappen, provincies en gemeenten landelijke afspraken gemaakt over extra waterberging. De uitvoering daarvan moet nu ingepast worden in de ruimtelijke ordening. Volgens planning is dit in 2015 gereed. Peter Glas: "Ik ben benieuwd of men in gemeenteraden en provinciale staten van het belang en de urgentie doordrongen is en of het overal gaat lukken. Zo niet, dan voorspel ik dat het water toch z'n eigen ruimte zal nemen, maar dan op plekken waar we het liever niet hebben. Waterbeheer heeft bovendien in bestuurlijke zin ruimte nodig. Ruimte om in te spelen op maatschappelijke behoeften die door de algemene democratie worden bepaald en om daar een acceptabel kostenniveau bij te realiseren. Ik pleit er voor om voortdurend kritisch te zijn op de uitvoering, scherp te zijn op de koers en kosten van het waterbeheer en zuinig op de organisatie en de bestuurlijke inbedding"

Beneden de grote rivieren
In Limburg hebben de waterschappen extra mensen ingezet voor controles. Er zijn demontabele wanden gebouwd, pomplocaties ingericht en (beek)mondingen afgesloten. De piekafvoer van de Maas werd op zaterdag 7 januari bereikt met een afvoer van 1670 m^3 per seconde bij meetpunt Sint Pieter. De afvoeren in de Maas en de beken hebben nergens tot problemen geleid. Er is intensief gecommuniceerd met de burgers en de media via de website en twitter.

Enkele feiten
Wetterskip Fryslan voerde 21 miljoen kubieke meter water af, ongeveer twee keer de inhoud van het Sneekermeer.
Waterschap Hunze en Aa's had ten tijde van de wateroverlast 325 mensen aan het werk, waarvan er meer dan 300 op pad waren om dijken en gemalen te controleren.
Zo'n 60 binnenschepen lagen vast vanwege het vaarverbod in Groningen en Friesland.
De R.J. Cleveringsluizen bij Lauwersoog hebben in één spuibeurt 18,3 miljoen kuub water gespuid. Dit zijn ruim 7000 tankauto's gevuld met water.
Waterbergingen in Drente en Groningen hebben ruim 355.000 kuub water kunnen bergen. Het peil van het Eelderdiep en het Peizerdiep daalde respectievelijk met 30 en 15 centimeter na het vol lopen van waterberging Peizer- en de Eeldermaden.

Wouter Jong,
adviseur crisisbeheersing Nederlands Genootschap van Burgemeesters

Rationele communicatie in een rationele crisis

Ongeveer 800 mensen en 2200 stuks vee moesten op 6 januari het gebied rond Woltersum en Wittewierum verlaten, omdat de dijk bij het Eemskanaal het bijna begaf. Het was een nacht waarin hulpverleners en bewoners zij-aan-zij stonden om de dijk te verstevigen met zandzakken.

De crisiscommunicatie tijdens het hoogwater wordt op dit moment nog geëvalueerd in een leerarena van de regio. Alle betrokkenen zullen hun licht laten schijnen op de punten die goed en minder goed gingen in die bijzondere uren en dagen. Maar afgaande op diverse media lijkt de conclusie gerechtvaardigd dat de communicatie van de evacuatie rond Woltersum op hoofdlijnen goed is verlopen. Via de eigen informatiekanalen en RTV Noord werden betrokkenen afdoende op de hoogte gehouden van de ontwikkelingen in het gebied en aan de dijk van het Eemskanaal.

Wanneer de communicatie inhoudelijk wordt bekeken, valt op dat het in deze crisis vooral draaide om informatievoorziening. Het lijkt in strijd met de gangbare teneur die de laatste jaren is ontstaan, waarin een burgemeester situaties vooral moet duiden en moet aanhaken bij de emoties van de bevolking. De duiding geeft op een hoger abstractieniveau aan hoe de samenleving met de schok omgaat. Het plaatst de crisis als het ware in een context. Dat is een passende strategie in situaties waarin een gemeenschap emotioneel van de kaart is. Een gezinsdrama, zedenzaak of andere schokkende gebeurtenis zal in veel gevallen vragen om een burgemeester die de emoties benoemt.

Maar deze crisis liet zien dat het beteugelen van emoties geen dogma moet worden. In de hoogwatersituatie was het 'duiden' nauwelijks nodig. Inwoners van het gebied reageerden behoorlijk laconiek op de hele situatie. Al je goed naar de burger luisterde, bleek men vooral concrete antwoorden te willen op vragen als 'waar gaat er nu gebeuren?' en 'hoe lang duurt het nog?' Dat werd in media afgedaan als 'typische Groninger nuchterheid', maar het zegt waarschijnlijk meer over het type crisis dan over de bevolking. Emoties als 'ontreddering' en 'angst' voerden in deze crisis niet de boventoon. Dan moet een burgemeester niet 'duiden om het duiden'.

In de bewonersbijeenkomst die na afloop op 16 januari in de Tiggelhal in Ten Boer werd georganiseerd, gaf burgemeester Van de Nadort aan dat de nuchterheid niet betekende dat de evacuatie bij iedereen in de koude kleren ging zitten. Bij menigeen zal de angst er goed in hebben gezeten toen de ME middenin de nacht aan de deur kwam om mensen aan te sporen binnen een half uur te vertrekken. Maar toen de eerste schrik was weggezakt bleven vooral de vragen over. Vragen over het hoe-en-waarom van de evacuatie, de dijk en de te nemen maatregelen. Die vragen zijn waar mogelijk beantwoord, inclusief de concrete instructies voor de bevolking (wat moeten we doen en laten om de crisis niet groter te maken dan deze al is?).

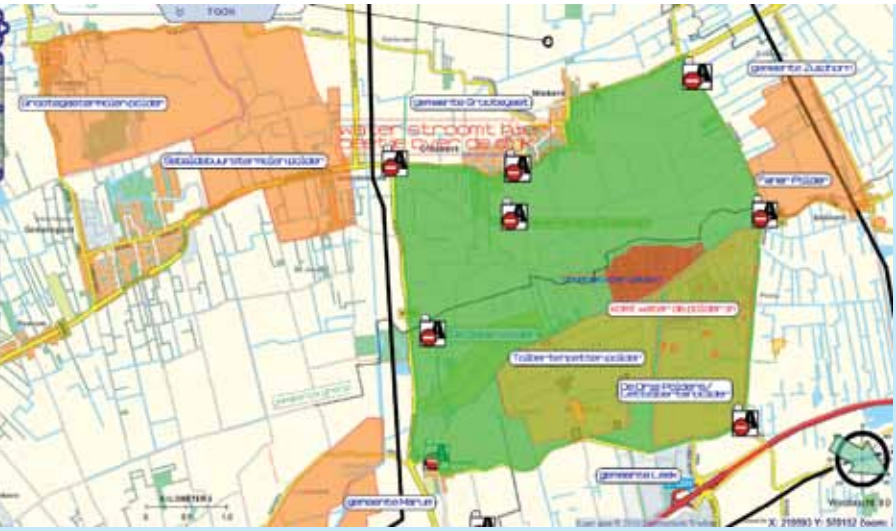
Resumerend moet een burgemeester emoties duiden als die er zijn. Maar als het qua emoties zo'n vaart niet loopt, ligt er op andere vlakken nog voldoende werk voor een burgemeester. Zoals de zwaarwegende besluiten om al dan niet te evacueren en noodbevoegdheden in te zetten. Diegenen die de burgemeestersrol bij crises reduceren tot 'boegbeeld en burgervader die de schok moet duiden' doen zowel de burger als de functie van de burgemeester in de crisisbeheersing tekort.

Rob Jastrzebski,
freelance journalist

Storm en wateroverlast hielden crisismanagers in delen van Noord- en West-Nederland begin januari dagenlang bezig. Groningen was het epicentrum van de gebeurtenissen, met evacuaties in de Tolberterpettenpolder en Woltersum. Grip 4 in de polder! Behalve water stroomde er in de getroffen gebieden ook rijkelijk informatie. Het netcentrisch werken kon in deze interregionale hoog-watersituatie zijn kracht tonen en deed dat ook.

"Regio's groeien in het gebruik van crisismanagementsysteem"

LCMS toont kracht tijdens wateroverlast



Vier dagen crisismanagement met het Landelijk Crisis Management Systeem (LCMS), voor het Regionaal Operationeel Team van de Veiligheidsregio Groningen was het een forse praktijkbeproeving van de capaciteiten van het systeem. En volgens Hans Foekens, een van de voorzitters ROT tijdens de hoogwaterepisode, kwam de functionaliteit in meerdere opzichten goed tot zijn recht.

Backbone

"Rust en overzicht kenmerkten de werksituatie in het team", blikt Foekens terug. "Het CoPI, het ROT en het Regionaal Beleidsteam hadden door het *real time* delen van informatie voortdurend dezelfde kijk op de werkelijkheid. Het gebruik van het systeem verandert ook de vergaderroutine. In de oude situatie waren we in iedere vergaderronde al snel een half uur kwijt voor gezamenlijke beeldvorming. Nu stappen alle partners voorzien van de meest actuele informatie in het overleg. De vergaderingen worden daardoor meer toegespitst op de kernpunten en we kunnen ons meer concentreren op feitelijke beslissingen en scenarioanalyse."
De netcentrische werkwijze is volgens Foekens ook een grote steun bij de aflossing van teamleden tijdens langduriger crises. In Groningen waren er tijdens de vier dagen durende hoogwatersituatie circa tien aflossingsmomenten. Foekens nam driemaal de rol van voorzitter ROT op zich. "Het briefen van nieuw instromende teamleden ging veel vlotter dan voorheen, omdat zij zich snel konden inlezen in de stand van zaken en openstaande aandachts- en beslispunten. LCMS houdt de informatie vast dwars door alle overdrachtsmomenten heen. Wij beschouwen het systeem dan ook als de informatiebackbone in onze crisisorganisatie."

Grafische plot

Liesbeth Post heeft dezelfde ervaringen. Ook in haar functie als informatiemanager van het ROT ervaart zij de snelheid van informatiedeling als een van de grootste winstpunten. "In de situatie vóór LCMS moest ik eerst alle secties langs om de actuele informatie op te halen en die samen te voegen tot een samenhangend geheel. Nu ontstaat dat gedeelde beeld vanzelf door de rechtstreekse input vanuit de secties. Ik kan mijn aandacht daardoor meer concentreren op aspecten als: 'Is de gepresenteerde informatie duidelijk genoeg voor alle partners en klopt het?' Als informatiemanager moet je wel scherp blijven op de inhoud. LCMS werkt uitstekend mits je informatie kort en bondig houdt. Géén lange tekstuele situatieschetsen, maar korte heldere feiten. Daarbij werken de 'bullits' in de informatieschermen mooi structurerend. Ook de grafische plot wordt door de gebruikers als een waardevolle functie ervaren. Vooral voor bestuurders heeft die plotfunctie meer-

waarde, omdat het hen helpt snel zicht te krijgen op bestuurlijke consequenties. Ze zien in één oogopslag waar de gemeentegrenzen lopen en waar de belangrijkste zwaartepunten liggen voor het gebied waarvoor zij bestuurlijk verantwoordelijk zijn."
Wat de gebruikers volgens Post nog wel moeten leren, is dat ze rigoureus oude informatie moeten weggooien, zodat het systeem alleen de meest actuele informatie laat zien. "Verouderde informatie vervuilt het systeem en doet afbreuk aan het overzicht. Weg is niet weg, want voor evaluatie achteraf wordt de hele informatiegeschiedenis van het incident in een diepere laag van het systeem bewaard."

Evaluatie

Veiligheidsregio Groningen gaat het gebruik van LCMS als onderdeel van het crisismanagement tijdens de wateroverlast grondig evalueren. Foekens en Post verwachten dat daar nog wel leerpunten uitkomen om het systeem nog efficiënter te kunnen gebruiken. Foekens: "We zijn nog lerende. Netcentrisch werken en LCMS als instrument zijn in juli vorig jaar in onze regio ingevoerd. We zijn er naar ons gevoel in geslaagd om het systeem door goed beheer en veel oefening en training een plek te geven binnen onze regionale crisisbeheersingssystematiek. We hebben het systeem al enkele keren in GRIP-situaties gebruikt. De langdurige inzet tijdens de wateroverlast heeft ons nadrukkelijk de grote voordelen laten zien van LCMS als informatiemanagement systeem tijdens crises. De praktijk is en blijft de beste leerschool."

Landelijk beeld

Ook op het nationale niveau kwam de meerwaarde van LCMS goed uit de verf. In het Landelijk Operationeel Coördinatiecentrum (LOCC) in Driebergen werden de ontwikkelingen in Noord-Nederland al enkele dagen op de voet gevolgd toen op donderdag 5 januari het besluit werd genomen om formeel op te schalen. Het LOCC trad in zijn rol als 'facilitator' van de regio's en het nationale niveau qua informatievoorziening en bijstandscoördinatie. Daarbij was LCMS volgens Bram de Nood, hoofd van de sectie Informatie, een belangrijke steun.
"Doordat we via LCMS de actuele situatie in de regio's *real time* konden volgen, konden we snel in onze rol komen. Onze eerste opgave was het samenstellen van een landelijk operationeel beeld en dat te delen met de andere regio's en het nationale niveau. Later kwam daar ook de bijstandscoördinatie rond de inzet van onder andere defensiecapaciteit en mobiele eenheid bij. Ook hier droeg het systeem bij aan overzicht. Alle betrokken regio's hadden continu overzicht van de gevraagde en geleverde capaciteit en bijstandverlenende regio's konden door de gepresenteerde inzetplanning ook anticiperen op het organiseren van hun bijstandseenheden."
De Nood ziet in het verloop van de informatiestromen het bewijs dat de regio's en het LOCC groeien in het gebruik van LCMS en daarvan ook steeds nadrukkelijker de meerwaarde onderkennen. "Het systeem brengt relatieve rust in een hectische situatie. Doordat informatie *real time* gedeeld wordt, hoeft er minder heen en weer gebeld te worden door crisisteams om zaken te checken of statusinformatie over bijvoorbeeld bijstandseenheden door te geven".
Volgens Neil Jordan, coördinator bij de sectie Informatie en informatiemanager tijdens de wateroverlast bij het LOCC, blijft duiding van informatie altijd nodig. Maar in het delen van operationele informatie heeft het systeem zijn kracht in termen van snelheid en overzicht tijdens de wateroverlastsituatie zeker bewezen.
Om het landelijk beeld compleet te maken, kon het LOCC niet uitsluitend bouwen op de informatiestroom uit LCMS, omdat nog niet alle regio's operationeel gebruik maken van het systeem. Deels moest dan ook informatie uit andere bronnen worden verkregen, met behulp van bijvoorbeeld e-mail en telefonisch contact. Jordan: "Het LOCC vulde de informatie vanuit de regio's aan met onder andere het landelijk weer- en verkeersbeeld, om vervolgens een bondig landelijk totaalbeeld beschikbaar te stellen aan de regio's en het nationale niveau. Twee dagen lang, continu up to date. Jordan: "De informatiebehoefte in het land was kennelijk groot, want op het piekmoment van de hoogwatersituatie volgden zestien regio's het landelijk beeld via LCMS. Het systeem heeft ons echt geholpen bij de uitvoering van onze taken. Doordat regio's het systeem vanaf het begin van een crisis goed vullen en continu *up to date* houden, kunnen wij de regio's op hun beurt ook weer goed proberen te faciliteren."

Onzekerheid als blinde vlek in het Europese Seveso-regime

Esther Versluis, universitair hoofddocent, Universiteit Maastricht
Marjolein van Asselt, hoogleraar Risk governance, Universiteit Maastricht raadslid, Wetenschappelijke Raad voor het Regeringsbeleid (WRR)

Een serie zware ongevallen in de Europese chemische industrie in de jaren zeventig leidde tot een vraag vanuit het Europees Parlement om de risico's van dit type zware ongevallen Europees te gaan reguleren. Na drie jaar onderhandelen zag in 1982 de eerste 'Seveso-richtlijn' het licht – vernoemd naar de plaats in Italië waar het op dat moment laatste zware ongeval had plaatsgevonden (1976). Het doel van de Seveso-richtlijn is om ongevallen te voorkomen en de schade voor mens en milieu te beperken indien zich toch een ongeval voordoet. Chemische bedrijven die door de hoeveelheid chemische stoffen die ze in huis hebben onder de richtlijn vallen, zijn verplicht uitgebreid te rapporteren over hun beleid en praktijk aan de hand van veiligheidsbeheerssystemen en uitgebreide scenario-exercities in veiligheidsrapporten.
Sinds de Seveso-richtlijn van kracht is, hebben toch meerdere zware ongevallen plaatsgevonden, en steeds hebben deze ertoe geleid dat de regels werden aangepast. De aanscherping van de richtlijn na de vuurwerkramp in Enschede is hier een voorbeeld van. Na twee amendementen (1987 en 1989), een volledige herziening van de richtlijn (Seveso II in 1996) en nog weer een amendement (2003), zijn intussen de onderhandelingen over een nieuwe 'Seveso III' in volle gang. Dit lijkt te suggereren dat het steeds opnieuw aanscherpen van richtlijnen de beste manier is om dit type zware ongevallen te reguleren. Op basis van de analyse van de aanpassingen concluderen wij dat in het Seveso regime de beleidsmakers voornamelijk bezig zijn met het managen van de ongevallen van gisteren, met als gevaar dat toekomstige (onzekere) risico's over het hoofd worden gezien.

Onzekerheidsblindheid in het Seveso regime?

De focus op reeds gebeurde ongevallen lijkt te worden ingegeven door de manier waarop risico's worden benaderd in het Seveso regime. De gehanteerde risicodefinitie verwijst naar de klassieke positivistische benadering, waarin risico's als voldoende calculeerbaar en controleerbaar worden beschouwd. Het wordt echter steeds breder erkend dat risico overloopt in onzekerheid. Sommige risico's zijn 'simpel': er is voldoende statistiek om die bedreigingen te berekenen als een functie van waarschijnlijkheid en effect (denk aan auto-ongelukken). In de gevallen waarin de omstandigheden en/of gevolgen onzeker zijn, omdat het bijvoorbeeld gaat om nieuwe technologieën, is er geen statistische basis om waarschijnlijkheid en impact in te schatten. Dergelijke "onzekere risico's" zijn niet of hooguit met heel veel slagen om de arm in een getal uit te drukken. De belangrijkste reden om het onderscheid te maken tussen simpele risico's enerzijds en onzekere risico's anderzijds, is omdat ze een verschillende aanpak qua beoordeling, management en communicatie vereisen. De in het Seveso-regime gehanteerde risicodefinitie suggereert dat ongevallen in de chemische industrie per definitie simpele risico's zijn. Dit kan uitmonden in 'blindheid' voor mogelijke onzekere risico's, met alle gevolgen van dien.

Onzekerheidsblindheid in de Nederlandse praktijk?

Dat de focus op calculeerbare risico's niet alleen op papier in de Seveso richtlijnen bestaat, maar ook in de Nederlandse praktijk, blijkt na het spreken van inspecteurs (12) en respondenten bij chemische bedrijven (8). Zo vertelde een inspecteur: 'Er zitten twee kanten aan risico's: kans en effect. Als je grote effecten hebt binnen een scenario gaan we behoorlijk aan de kans werken'. En een vertegenwoordiger van een chemische multinational zei: 'Eerst worden ze [de risico's] gekwantificeerd en dan geclassificeerd'. Ook de

Nederlandse aanvulling in de omzetting van de Europese Seveso-richtlijn naar Nederlandse wet- en regeling van het concept 'restrisico's' wijst op een klassiek positivistische benadering. Een van de geïnterviewde inspecteurs verwoordde het als volgt: 'Restrisico's zijn een uitspraak over het feit dat je van te voren weet dat je een bepaalde ramp met een bepaalde omvang gewoon niet kunt behandelen. Het is een theoretisch model, er is een risico dat je accepteert'. Restrisico's worden geaccepteerd: de aanname is dat het onwenselijk is om ze te managen omdat dit te duur is, in absolute zin of relatief (in verhouding tot de veiligheidswinst). Door het gebruik van de term 'rest' (zoals in restafval) wordt gesuggereerd dat deze risico's onbelangrijk zijn vanuit een risicoreguleringsperspectief. Door risico's met een zeer kleine kans en onberekenbare, oncontroleerbare risico's te presenteren als 'rest' wordt deze categorie, en daarmee onzekerheid, gemarginaliseerd of zelfs buiten het blikveld geplaatst.
Ook heeft de Nederlandse omzetting van de Seveso richtlijnen in het Besluit Risico's Zware Ongevallen de focus op het calculeren van risico's vergroot. De Nederlandse omzetting verplicht chemische bedrijven een kwantitatieve risicoanalyse te doen. Dat is een verplichting die niet door de Europese regelgeving wordt vereist.

Van onzekerheidsblindheid naar onzekerheidstolerantie

Iedere verandering in het Seveso regime is een reactie op een ongeval in de chemische industrie. Hoewel we zeker niet willen beweren dat het onverstandig is om te leren van het verleden, willen we wel benadrukken dat dit niet voldoende is om toekomstige ongevallen te voorkomen of er ten minste op voorbereid te zijn. Als we iets kunnen leren van de serie ongevallen in de chemische industrie, dan is het wel dat zich juist onvoorziene scenario's met zware gevolgen voordoen. Zonder de uitzonderingen tekort te willen doen – een aantal geïnterviewden toonden zich zeker bewust van onzekerheden – kunnen we stellen dat er een neiging bestaat om onzekere risico's binnen het Seveso regime niet aandacht te geven die ze verdienen. Risico's worden teveel gepresenteerd en gepercipieerd als simpel, calculeerbaar en dus controleerbaar. Beperkingen aan de calculeerbaarheid en controleerbaarheid worden door enkele inspecteurs en bedrijven wel gesignaleerd, maar over het algemeen wordt onzekerheid niet erkend in het Seveso regime.
Onzekerheid is een blinde vlek in het Seveso regime. Simpelweg een nieuw managementsysteem biedt voor het omgaan met onzekerheid waarschijnlijk onvoldoende soelaas. Er lijkt een cultuurverandering nodig te zijn in het denken over risico's in de chemische sector. Het huidige systeem is zeer op regelgeving georiënteerd. Er is meer aandacht nodig voor het onderzoeken en stimuleren van onzekerheidstolerantie bij chemische bedrijven. Hoe wordt over risico's nagedacht? Welke lessen worden er getrokken uit het verleden? Worden onzekere scenario's verkend? Welke conclusies worden daaruit getrokken? Wat betekent een onzekerheidstolerante houding voor de dagelijkse praktijk binnen een bedrijf? Inspecteurs zouden een belangrijke rol kunnen spelen in het verhogen van het onzekerheidsbewustzijn van bedrijven.
Het is een illusie om te denken dat onzekerheidstolerantie garandeert dat ongelukken worden voorkomen. Maar een gewaarschuwd mens telt voor twee: elk ongeluk dat voorkomen wordt of beter wordt beheerst, is een bijdrage aan de fysieke veiligheid gezien de maatschappelijke schade die een zwaar ongeval in de chemische industrie meestal met zich mee brengt. En een andere manier van omgaan met risico's is niet per definitie duurder, zeker gelet op de administratieve lasten die het huidige Seveso regime met zich meebrengt, dus het lijkt de moeite van het uitproberen waard. En het Seveso III proces biedt daartoe mogelijk ook kansen.

Referenties

E. Versluis, M. van Asselt, T. Fox and A. Hommels, 'The EU Seveso regime in practice. From uncertainty blindness to uncertainty tolerance', in: *Journal of Hazardous Materials*, 184 (2010), 627-631.
Wetenschappelijke Raad voor het Regeringsbeleid, *Onzekere Veiligheid*, 2008.

dr. Vincent van der Vlies,
adviseur veiligheid, ARCADIS
(Vincent.vandervlies@arcadis.nl)

Evenwichtskunst van de WRR: een reflectie

Eind november vorig jaar publiceerde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het rapport *Evenwichtskunst*. Aanleiding was een verzoek uit april 2011 van de Minister van Binnenlandse Zaken en Koninkrijksrelaties om een reflectie te schrijven over, en een visie te formuleren, op de mogelijkheden voor een generiek risicobeleid op het gebied van de fysieke veiligheid. Concreet waren de vooraf gestelde centrale vragen: Welke mogelijkheden ziet u voor een generiek risicobeleid met een kleinere rol voor de overheid met betrekking tot het afwenden en compenseren van risico's? In hoeverre ziet u aanknopingspunten om bestaande mechanismen te doorbreken en blokkades weg te nemen, zowel wat betreft de risico-regelreflex, als wat betreft de reflex om de verantwoordelijkheid bij de overheid te leggen?

Uit deze vragen ontspint een buitengewoon interessant en belangwekkend stuk, waarin de WRR lijkt te worstelen met de complexiteit van de gestelde vragen en de gehanteerde begrippen. Risico's worden gedefinieerd als calculeerbare veiligheidsproblemen, overigens een andere definitie dan in het WRR rapport *Onzekere veiligheid*, maar het rapport geeft ook aan dat er een geleidelijke overgang van risico's naar onzekerheid bestaat die eveneens de fysieke veiligheid kan bedreigen. Bij onzekerheid gaat het dan om dreigingen die niet vaststaan, maar waarbij incidenten en schadelijke gevolgen wel denkbaar zijn. Deze terechte opmerking maakt het rapport qua generaliseerbaarheid echter ingewikkeld te doorgronden, omdat het nu soms schimmig blijft waarover men spreekt: risico's, onzekerheden of toch incidenten?

De WRR stelt – terecht – dat als er al een reflex lijkt te zijn op het gebied van risicoregels, dit eerder op het gebied van incidenten is en het gerechtvaardigd lijkt om te spreken van een incidentregelreflex. Dit gaat gepaard met de opmerking dat er bij gebrek aan empirisch onderzoek naar de politiek-bestuurlijke follow-up van incidenten het de vraag is aan welke voorbeelden waarde moet worden gehecht en 'de publicaties (...) over de veronderstelde incidentenreflex hebben naar ons oordeel een te hoog anekdotisch en essayistisch karakter'. De WRR geeft aan dat in het kader van de Vuurwerkramp het beleid werd aangescherpt, maar verder zijn er geen zaken bekend waarbij dit eveneens gebeurde. Hier wordt naar mijn mening teveel voorbij gegaan aan de milieuregels die zijn ingesteld naar aanleiding van gezondheidsrisico's; te denken valt aan allerlei zaken: van roetfilters tot fosfaatregelingen en van het afschaffen van cfk's tot bodemsanering. Allemaal voortgekomen uit observaties en incidenten, waarvan erkend werd dat deze een nadelig gevolg hadden op de menselijke veiligheid.

Voorts behandelt men in het derde hoofdstuk risico's en onzekerheid als begrippen, waarbij een handreiking wordt gegeven van vijf aanknopings- en aandachtspunten, te weten: het vervlechten van goede en kwade kansen, het verdisconteren van sociaal-psychologische

kenmerken van gevaar, het benutten van risicovergelijkingen, het accepteren van onzekerheid en het organiseren van de omgang met onzekerheid. Stuk voor stuk goede uitgangspunten, maar deze komen uit de lucht vallen en hier had meer reflectie en uitleg moeten volgen over het weglaten van andere mogelijke punten.

De zeer interessante analyse over schade vormt wat mij betreft een verrijking van de studie. Ik ben het met de auteurs eens dat de schade van incidenten niet eenzijdig bij de overheid zou moeten komen te liggen. De analyse maakt terecht opmerkingen over de 'kale kip' die bijvoorbeeld in Moerdijk boven kwam drijven. Een actor veroorzaakt een risico en uiteindelijk draait de maatschappij voor de kosten op, zonder dat de actor compenseren kan. In deze analyse wordt helaas slechts kort de rol van vliegmaatschappijen aangehaald die volgens de WRR 'genoemd en geroemd' worden als voorbeeldsector. Hier had ik graag gezien wat wij van hen kunnen leren en of er geen regelingen te bedenken zijn die generiek toepasbaar zijn. Ook is het belangrijk om je af te vragen of het niet te simpel is om te stellen dat private risicoveroorzakers alle schade moeten verzekeren. Vanuit een rechtvaardigheidsperspectief zeg ik uiteraard ja. De praktijk zal ongetwijfeld een stuk complexer blijken. Stel bijvoorbeeld dat een vervoerder van gevaarlijke stoffen over het spoor verantwoordelijk gesteld wordt voor de explosie van een tankwagon met LPG op een druk station als Utrecht Centraal. Hoeveel kosten dit met zich meebrengt valt niet te zeggen en wie kan of wil zoiets verzekeren?

Terecht wordt opgemerkt in de conclusie dat een generiek systeem voor schadevoorzieningen niet mogelijk is. Desondanks roept de WRR niet op tot een discussie over de wenselijkheid van generiek beleid an sich. Iets wat voor een dergelijke analyse wat mij betreft had gemoeten. Is het dan 'verstandig (…) om incidentenpolitiek centraal te stellen in het denken over verantwoordelijkheid voor fysieke veiligheid' vraagt de WRR zich retorisch af. Mijn antwoord hierop is – uiteraard – nee. De door de WRR aangegeven structurele onderzoeksplicht en omkering van de bewijslast naar risicoveroorzakers, lijken mij daarom goede methoden om onzekerheden af te dekken. Hierbij verschuift de aandacht van de gevolgen van de mogelijke innovatie zelf, naar hoe om te gaan met de negatieve externaliteiten die de innovatie met zich meebrengt. Dit opent enerzijds de deur voor een specifiek risicobeleid wat naar mijn mening en ervaring vaak beter werkt, omdat risico's en onzekerheid zich niet laten kenmerken door generieke kansen en gevolgen. Anderzijds geeft deze houding blijk van erkenning van de onkenbaarheid van sommige gevolgen.

Hier valt echter wel iets tegen in te brengen. Om dit te duiden is het goed om uzelf in een gedachtenexperiment de vraag te stellen wat u zou doen wanneer nu de verbrandingsmotor zou worden uitgevonden: zou u, als politicus destijds de voor- en nadelen overwegende, deze verbieden als u te horen zou krijgen dat buiten de voordelen ook grote vele honderden doden per jaar alleen in Nederland zouden vallen door deze uitvinding? Zou u dan tegen geweest zijn? Met andere woorden, de kennis die gegenereerd zal worden bij ex-ante analyses over goede en kwade kansen maakt dat er wellicht geen goede aanbevelingen gegeven kunnen worden, omdat wij dergelijke afwegingen niet objectief kunnen nemen en de evenwichtskunst hierdoor vervalt tot een onbalans in de richting van het ten onrechte mijden van kwade kansen.

Wat mij betreft vormt het rapport een waardevol startpunt voor verder onderzoek, maar het eindpunt is nog niet bereikt, omdat de materie te omvattend is om in alleen dit rapport te vatten. Ik zou daarom naast de aanbevelingen in het rapport ook onderzoek doen naar de mogelijkheden voor specifiek risicobeleid, of en hoe een objectief afwegingskader gecreëerd kan worden dat goede en kwade kansen afweegt en wat geleerd kan worden van de instelling van het milieubeleid vanaf de jaren 70 tot nu.

Barry van 't Padje,
onderzoeker en senior adviseur Crisislab,
(b.vantpadje@crisislab.nl)
Andrea Naphegyi,
adviseur risicocommunicatie veiligheidsregio Utrecht,
(A.Naphegyi@vru.nl)

Risicocommunicatie door de overheid
Wat de burger écht verwacht

Met de inwerkingtreding van de Wet veiligheidsregio's is risicocommunicatie (ook) een taak van de veiligheidsregio geworden. De veilig-heidsregio Utrecht (VRU) wilde voor deze taak een beleidsplan opstellen dat mede gebaseerd zou zijn op de verwachtingen van de burger uit de regio Utrecht. De VRU gaf Crisislab[1] de opdracht om deze verwachtingen in kaart te brengen, in het bijzonder voor de risico's uit het regionale risicoprofiel.

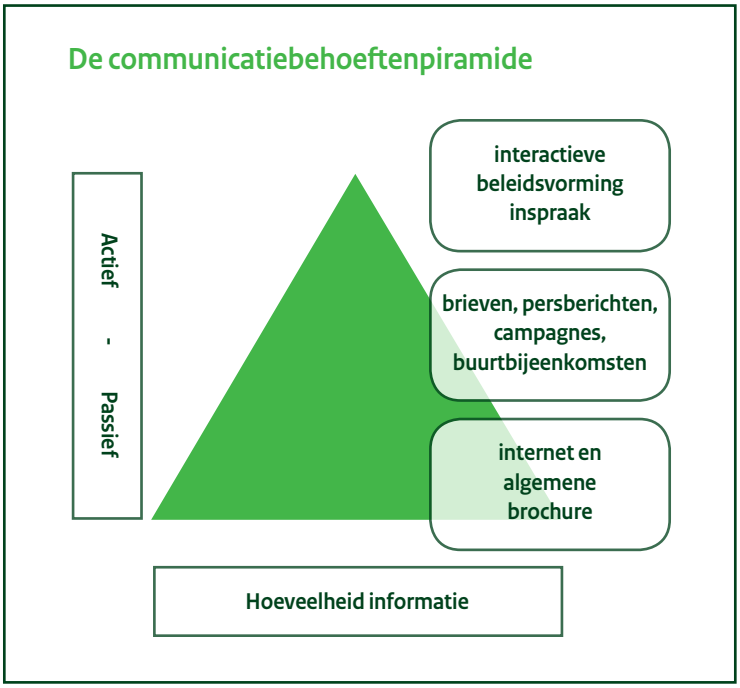
Het onderzoek
De risico's uit het risicoprofiel van de VRU stonden centraal in het onderzoek. Dit zijn allemaal zogenaamde 'kleine-kans-groot-effect-risico's', oftewel situaties en gebeurtenissen die meestal veilig zijn, maar als ze mis gaan zeer ernstige gevolgen hebben. Het onderzoek ging over wat de burger van de overheid verwacht qua communicatie over deze potentiële rampen en crises. Eerst is er via 250 straatinterviews een representatief beeld verkregen van de risicoperceptie van de Utrechtse burger. Vervolgens is via focusgroepen onderzocht wat deze burgers verwachten van de overheid op het gebied van risicocommunicatie.

De resultaten
De meest algemene verwachting van de burger is dat overheden integer handelen en communiceren. Deze algemene verwachting is opgebouwd uit vijf inzichten. Deze vijf inzichten vormen de rode draad van het Visiedocument Risicocommunicatie 2012 – 2015 van de veiligheidsregio Utrecht en worden hieronder gepresenteerd.
Burgemeester Ties Elzenga (gemeente Veenendaal): 'Voor mij is het belangrijkste inzicht uit het onderzoek dat voor het behalen van de beleidsdoelen het van groot belang is dat de burger zijn overheid vertrouwt. Door de 'inzichten' te volgen kunnen we het vertrouwen vergroten.'

Inzicht 1: hanteer een terughoudende, informerende communicatiestijl
Uit het onderzoek blijkt dat de risicoperceptie van de burger realistisch is. De burger stelt terecht dat de dreiging van rampen en crises relatief klein is. De burger maakt zich daarom niet echt zorgen over het risicoprofiel van de regio Utrecht. Dit tempert de behoeften aan risicocommunicatie en rechtvaardigt een enigszins terughoudende communicatiestijl van de overheid. In algemene zin zit de burger niet te wachten op een overheid die hem probeert te overtuigen dat hij bepaalde voorzorgsmaatregelen moet nemen. De burger vindt een informerende communicatiestijl het prettigst. Inhoudelijk gezien is hier weinig tegen in te brengen omdat de risico's relatief klein zijn en de burger ze niet onderschat. Als de burger de risico's uit het regionale risicoprofiel al niet goed inschat, dan betreft dat vrijwel altijd een overschatting. Voor een deel van de risico's uit het risicoprofiel van de regio Utrecht is dit in lichte mate het geval. Voor deze risico's kan volgens Crisislab een meer consulterende communicatiestijl overwogen worden.

Inzicht 2: speel in op een dynamische behoefte aan risicocommunicatie
Uit het onderzoek blijkt dat de burger vindt dat de overheid over risico's moet communiceren wanneer de boodschap voor de burger praktisch nut kan hebben of omdat door een verandering in het risico of het risicobeleid zijn belangen in het geding zijn. Als risicocommunicatie niet praktisch nuttig is of niet in gaat op zijn belang dan heeft de burger er weinig behoefte aan. Een passieve informatievoorziening via internet en brochures is dan volgens de burger voldoende.
Burgemeester Elzenga: 'Een ingewikkeld dilemma vind ik de tegenstrijdigheid tussen enerzijds een terughoudende informerende communicatiestijl en anderzijds het actief omgaan met het dynamische karakter van risicocommunicatie. Het laatste vraagt juist geen terughoudendheid.'

[1] De stichting Crisislab is de onderzoeksgroep die het onderzoeksprogramma van de leeropdracht Besturen van Veiligheid van de Radboud Universiteit Nijmegen ondersteunt.



Inzicht 3: doe niet net alsof

De burger verwacht dat de overheid realistisch is. Dit betekent dat de overheid zowel zou moeten vertellen over de successen die zij boekt via haar risicobeleid als over de tekortkomingen en de belangentegenstellingen waar zij mee te maken heeft. De burger wil geen geruststellende boodschappen horen, maar feitelijke informatie ontvangen.
Overheden moeten volgens de burger nooit meer veiligheid garanderen dan de burger zelf verwacht. Vrijwel alle burgers in de regio Utrecht (92%) verwachten dat de overheid niet alle risico's kan wegnemen en dat ongelukken en rampen altijd kunnen gebeuren. Door net te doen alsof er niets aan de hand is en er geen bedreigingen zijn voor de veiligheid, wordt de indruk gewekt dat de overheid iets probeert te verbergen. Burgemeester Mark Röell (gemeente Baarn): 'Onze burgers willen eigenlijk een risicoloze maatschappij, maar een opvallende constatering van het onderzoek is dat zij risico's wel degelijk accepteren.'

Inzicht 4: stel eigen verantwoordelijkheid van de burger centraal

Veruit het grootste deel van de burgers in de regio Utrecht (87%) voelt de verantwoordelijkheid om zich op rampen en ongelukken voor te bereiden. Hij bereidt zich echter alleen voor als het in zijn ogen oog zinvol is. De risico's uit het risicoprofiel zitten wat dat betreft in een lastig parket. Immers, het zijn relatief kleine risico's waar de burger bovendien maar weinig controle over heeft. De burger vindt het daarom zinvoller om zich voor te bereiden op meer alledaagse risico's, zoals brand. Er zijn volgens Crisislab wel kansen om dit enigszins te veranderen, maar dan moet wel de eigen verantwoordelijkheid van de burger centraal staan. De overheid zal zakelijk op de inhoud moeten overtuigen, zonder moreel appèl. Zij heeft de grootste kans dat dit lukt als zij met haar communicatie afstemt op de behoeften van burgers.

Burgemeester Röell: 'Ik vind het toch wel opvallend dat mensen heel duidelijk hun eigen verantwoordelijkheid voelen en weten dat ze zelf stappen moeten ondernemen om de eigen veiligheid te bewerkstelligen. En dat terwijl heel lang gedacht is in termen van eenrichtingsverkeer: wij moeten dat als overheid organiseren. Daarnaast blijkt dat burgers niet zitten te wachten op algemene campagnes waarin informatie wordt verstrekt, ze willen heel specifieke informatie. Men is veel meer op zoek naar specialisten, niet naar bestuurders. Dat de eigen verantwoordelijkheid zo duidelijk wordt gevoeld, is een heel goede ontwikkeling.'

Inzicht 5: hanteer een getrapt communicatiemodel

De burger verwacht dat de overheid via een getrapt communicatiemodel inspeelt op zijn behoeften. De onderste laag van het door burgers gewenste communicatiemodel wordt gevormd door een algemene, publieke informatievoorziening. De overheid zou volgens de burger moeten voorzien in objectieve informatie over risico's, het risicobeleid en de bijbehorende handelingsperspectieven. De burger moet de informatie die hij zoekt kunnen vinden via brochures, boekjes en vooral het internet.
De middelste laag wordt gevormd door een actief communicerende overheid die daarbij gebruik maakt van nieuwsmedia en eigen middelen. Deze laag treedt in werking als het risico en/of de beheersing van het risico verandert. De burger verwacht bijvoorbeeld dat informatie over een verhoogde kans op een natuurbrand en de daarbij horende handelingsperspectieven via de nieuwsmedia worden gecommuniceerd. Men wil zoveel mogelijk de informatie ontvangen via de kanalen die ze dagelijks gebruiken. Beleidsmatige veranderingen, bijvoorbeeld op het gebied van overstromingsrisico's, kunnen volgens de meeste burgers ook prima via de nieuwsmedia worden gecommu-niceerd. Sommige burgers stellen het op prijs als dit via specifieke overheidsmiddelen wordt gecommuniceerd, zoals een nieuwsbrief.
De bovenste laag is een direct communicerende overheid. Hier heeft de burger met name behoefte aan als zijn belang wordt geschaad. Als door het nieuwe beleid voor overstromingsrisico's de kelder van zijn huis vaker onder water zal staan, is communicatie via de nieuwsmedia niet meer afdoende. Dan verwacht hij dat dit persoonlijk aan hem wordt gecommuniceerd en dat er mogelijkheden zijn om vragen te stellen. Een andere belangrijke aanleiding om als overheid direct met een specifieke groep burgers te communiceren, is een locale overschrijding van bepaalde veiligheidsnormen. Dit is bijvoorbeeld het geval voor straling van elektriciteitsmasten en vervoer van gevaarlijke stoffen.

Het eindrapport is te downloaden op. www.crisislab.nl

Voorzitter Landelijke Operationele Staf bezoekt Thailand

Centrale coördinatie is vitaal

Op uitnodiging van de Thaise politie bracht Peter van Zunderd, voorzitter van de Landelijke Operationele Staf, van 14 tot en met 19 november een bezoek aan Bangkok. Hij liet zich informeren over de gevolgen van de ongekende watersnoodramp die het land trof en de maatregelen van de overheid.

Gijs Tra,
eindredacteur
KLPD Magazine

Wie hebt u tijdens uw bezoek ontmoet?
"Generaal Watcharapol van de Royal Thai Police introduceerde mij in augustus 2011 bij de directeur-generaal van het Department of Disaster Prevention and Mitigation (DDPM). We bespraken de rampenbestrijding en crisisbeheersing na de tsunami van 2004. Inmiddels was Thailand getroffen door de ernstigste overstromingen in vijftig jaar. Dit bezoek bood een goede gelegenheid om me te laten informeren over de omvang van de ramp en de aanpak door de Thaise overheid. Desgevraagd nam ik deel aan een geplande bijeenkomst van onze ambassadeur, Joan Boer, met de Thaise premier, mevrouw Yingluck. Evenals Adri Verwey van Deltares, die toen ongeveer zes weken werkte als adviseur van de Thaise regering op het vlak van watermanagement. Zijn zeer deskundige adviezen bespaarden Bangkok een overstroming van het zakencentrum."

Wat besprak u met de premier?
"Vooral een Nederlandse Inception Study voor de waterloop in Thailand, als fundament voor een structurele aanpak van dit probleem. Verder stond een samenwerking tussen onze landen op het gebied van watermanagement op de agenda. Ik lichtte daarbij op hoofdlijnen toe hoe Nederland de rampenbestrijdingencrisisbeheersing heeft georganiseerd. Ook kwam een Waterforum in Bangkok ter sprake. Begin 2012 delen Nederland en Thailand daar ervaringen met andere Zuidoost-Aziatische landen."

Welke indruk maakte de overstroming op u?
"Gesprekken en bezoeken gaven me een beeld van de omvang en de aanpak. De impact is uitzonderlijk: het overstroomde gebied is bijna zo groot als Nederland. Er kwamen 255 mensen om het leven. Naar schatting één miljoen mensen verloren hun huis. De overheid ving ongeveer 80.000 mensen op in shelters. De rest zocht zelf een onderkomen bij familie of bijvoorbeeld hoger gelegen bouwwerken zoals viaducten. De materiële schade valt nog altijd niet in cijfers uit te drukken. De Thaise bevolking ondergaat alles schijnbaar gelaten. Ze blijven zelfs in deze omstandigheden lachen, al verbergt hun lach veel spanning en stress. De hoge temperaturen voorkomen gelukkig levensbedreigende situaties door onderkoeling, zoals bij ons het geval zou zijn. Maar er heerst wel angst voor besmettelijke ziekten. Het Ministerie van Volksgezondheid is alert en neemt waar nodig maatregelen. Vooral schoon drinkwater heeft prioriteit."

Wat viel u als deskundige zoal op?
"Tijdens mijn bezoek aan het Flood Relief Operation Center constateerde ik versnippering. De belangrijkste ministers ontmoeten elkaar weliswaar dagelijks, maar elke partij lijkt zijn eigen gang te gaan. Zo valt de inzet van het Thaise leger – die traag op gang kwam, maar nu

goed verloopt – niet onder de civiele coördinatie. Daar gaan enkele generaals over. De minister van Justitie leidt het totaal. Niet op basis van enig plan, maar vooral omdat hij als oud-korpschef van de Thaise politie ervaring heeft met het aansturen van operationele eenheden.
Verder kreeg ik een goede indruk van de nazorg. Een callcenter met 80 fte's ontvangt 24/7 alle hulpvragen. Onduidelijk bleef wat daarmee gebeurt, al spelen lokale overheden wel een grote rol. Logistieke processen zijn uitermate belangrijk. Vooral transport over water. Het DDPM stelde duizenden (rubber)bootjes ter beschikking en je ziet vanzelfsprekend direct een levendige handel daarin. Het teruglopen van deze handel is vaak een teken dat de hoogste nood voorbij is."

Is er voldoende gedaan om de gevolgen te beperken?
"Het gaat om een zogenaamde *slow flood*. Het land stroomde van noord naar zuid langzaam vol over een breed gebied. De regering kon de bevolking dus tijdig waarschuwen, maar ik moest constateren dat zij op dat punt in gebreke bleef. Waarschuwingen kwamen te laat en waren niet afdoende. Dat veroorzaakte veel te voorkomen schade. Mensen konden hun bezittingen niet tijdig in veiligheid brengen. Vooral veel auto's gingen onnodig verloren. Voor de Thai een statussymbool, want ze kosten vaak meerdere jaarsalarissen. Hierover heerst veel ergernis en boosheid bij de bevolking, vooral omdat de verzekeringsmaatschappijen zeer waarschijnlijk niet uitkeren. De meeste polissen sluiten natuurschade uit."

Heeft de internationale gemeenschap voldoende bijgedragen?
"De Verenigde Staten doneerde tien miljoen dollar voor humanitaire hulp en verder hulppakketten met drinkwater en levensmiddelen. Andere internationale hulp zag ik niet. De Japanse regering ondersteunde alleen de eigen, door het water bedreigde bedrijven – uit economisch oogpunt. Tijdens gesprekken vertelde ik over het Water Search en Rescue Team dat sinds enkele maanden paraat is en via de Europese Unie kan worden aangevraagd. Dat team zou eventueel nog een bijdrage kunnen leveren aan de nazorg en bevoorrading van evacués."

Hoe is de situatie nu?
"De overstromingen zijn over het hoogtepunt heen. De regentijd is voorbij en het centrum van Bangkok blijft naar alle waarschijnlijkheid droog. Maar de nazorg vergt nog maanden. De Thai zijn volop bezig om toeristische trekpleisters zoals Ayutthaya grondig te reinigen. De tijdelijk gemetselde muren en de zandzakken verdwijnen van lieverlee uit Bangkoks centrum."

Welke leert de Thaise overheid van deze ramp?
"Mijn gesprekken met Thaise politici en deskundigen bevestigden het beeld van een trots land dat niet snel om hulp vraagt. Dat zagen we ook na de tsunami. Toch is Thailand beslist geïnteresseerd in onze waterhuishouding. Ook van de organisatie en uitvoering van onze rampenbestrijding willen ze graag leren. De ambassadeur nodigde de Thaise regering namens ons kabinet uit tot samenwerking op watermanagement gebied en een daaraan gerelateerd bezoek aan Nederland. Na overleg met de Nationaal Coördinator Terrorisme en Veiligheid heb ook ik de Thaise regering voorgesteld om hier te komen kijken hoe wij rampenbestrijding en crisisbeheersing organiseren."

Wat zijn uw conclusies na dit bezoek?
"Centrale coördinatie is vitaal bij het bestrijden van zo'n omvangrijke ramp. Onze multidisciplinaire aanpak door politie, brandweer, ambulancediensten, gezondheidszorg, gemeenten en defensie heeft grote waarde. Verder is goede afstemming van het centrale en decentrale gezag van het grootste belang. Een tijdige, heldere en vooral eerlijke communicatie is essentieel voor het vertrouwen van de bevolking in de overheid. Het ontbreken daarvan leidt tot eigenrichting. Zo staken woedende Thai zandzakdijken door, omdat het bij de buren droog bleef, terwijl hun bezittingen onderliepen. Nazorg vormt naast het bestrijden van de ramp wellicht de grootste overheidsopdracht. Die moet meteen starten en aandacht blijven krijgen. Dit vergt veel capaciteit, zowel in het publieke als in het private domein. En tot slot, maar zeker niet de minst belangrijke conclusie: we mogen internationale samenwerking en hulpverlening bij zo'n omvangrijke ramp beslist niet uit het oog verliezen."

Foto's: Ruud Jansen

Daan Weggemans,
Centrum voor Terrorisme en Contraterrorisme

Nieuwe Masteropleiding

‘Crisis and Security Management’

Per 1 februari is aan de Universiteit Leiden in Den Haag de nieuwe bestuurskundige master ‘Crisis and Security Management’ van start gegaan.

De bestuurlijke omgang met veiligheid is de afgelopen decennia drastisch veranderd. De traditionele noties van veiligheidsmanagement zijn gebaseerd op soevereine staten die verbonden zijn aan begrensde gebieden waarbinnen overheidsinstellingen als de politie, douane en inlichtingendiensten verantwoordelijk zijn voor het garanderen van de veiligheid.
Sinds de jaren negentig van de vorige eeuw wordt het gebied van veiligheidsmanagement echter in toenemende mate gekenmerkt door vergaande fragmentatie en diversiteit aan individuen en organisaties. Overheidsinstellingen krijgen steeds vaker te maken met publiekprivate, private, transnationale organisaties (met name de Europese Unie) en informele netwerken, waardoor het denken over veiligheid en het treffen van veiligheidsmaatregelen niet uitsluitend meer binnen het domein van de staat vallen.
‘Veiligheid’ lijkt een stopwoord geworden voor alle situaties en ontwikkelingen die door de samenleving als problematisch en bedreigend worden beschouwd. Met een focus op risico en preventie, is het veiligheidsbeleid in toenemende mate gericht op het aanpakken van alle mogelijke risico’s die binnen een samenleving bestaan. Daarmee is veiligheids- en risicomanagement een terrein geworden voor zowel publieke als private organisaties om objectieve en subjectieve ervaringen en percepties van onveiligheid en onzekerheden aan te pakken ter bevordering van stabiliteit, recht en orde in de samenleving.

Deze complexe relaties, ontwikkelingen en inzichten komen volop aan bod in de nieuwe master *Crisis and Security Management* (CSM): een opleiding specifiek gericht op de theorie en praktijk van crisisbeheersing en veiligheidsmanagement en een primeur voor Nederland en Den Haag. Binnen deze master vormen veiligheid, private beveiliging, crisiscommunicatie en (contra) terrorisme belangrijke thema’s. Vragen die aan bod komen zijn: Hoe heeft het denken over veiligheid en risico’s zich in de afgelopen decennia ontwikkeld? Wat kan de publieke sector leren van haar private partners op het gebied van innovatie, efficiëntie en effectiviteit? Hoe staat het met democratische controle en burgerrechten door de opkomst van nieuwe (private) spelers op de ‘veiligheidsmarkt’? Tevens worden enkele belangrijke aspecten van veiligheidsstrategieën nader bestudeerd – zoals de huidige en historische rol van inlichtingen- en veiligheidsdiensten (intelligence) binnen samenlevingen. Een andere belangrijk onderwerp is crisiscommunicatie. Met de opkomst van nieuwe sociale media heeft communicatie tussen autoriteiten en burgers er een extra dimensie bij gekregen. Ook zal er aandacht besteed worden aan specifieke verschijnselen als radicalisme en terrorisme. Welke verschillende verklaringen kunnen er bijvoorbeeld worden gegeven voor de motivaties en gedragingen van terroristen? En hoe kunnen we op basis van deze inzichten contraterrorismebeleid aanscherpen of achteraf evalueren?

In de masteropleiding wordt gezocht naar een evenwicht tussen academische kwaliteit en diepgang, en een meer praktische oriëntatie gericht op beleid en bestuur. Deze praktische oriëntatie werd ook tijdens de officiële opening benadrukt. De eerste lichting master-studenten bezocht het instituut voor Veiligheids- en Crisismanagement (COT), het Ministerie van Defensie, de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en sloot de eerste studiedag af met een presentatie bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Met de komst van deze masteropleiding is Den Haag niet alleen de stad waar politici, beleidsmakers en andere professionals zich over de complexe vraagstukken rond crises en veiligheid buigen, maar ook de plek waar op het hoogste academische niveau hierover onderwijs wordt gegeven.

Colofon

Redactieadres Magazine nationale veiligheid en crisisbeheersing
Ministerie van Veiligheid en Justitie
Kamer H1420
Postbus 20301
2500 EH Den Haag
E-mail: crisisbeheersing@minbzk.nl

Redactie
Redactiecommissie: Ruth Clabbers, Esther de Kleuver, Chris van Duuren, Marja Gobert, Donna Landa, Judith Sluiter, David van Veenendaal en Geert Wismans (samenstelling en eindredactie)
Redactiesecretariaat: Nalini Bihari (070-426 53 00)

Redactieraad
Prof. dr. Ben Ale (Technische Universiteit Delft)
Prof. dr. ir Marjolein van Asselt (Universiteit Maastricht, Wetenschappelijke Raad voor het Regeringsbeleid)
Prof. dr. Edwin Bakker (Universiteit Leiden/ Centre for Terrorism & Counterterrorism)
Prof. dr. Arjen Boin (Universiteit Utrecht)
Mr. dr. Ernst Brainich
Prof. dr. Adelbert Bronckhorst (TNO/VU Amsterdam)
Dr. Menno van Duin (Nederlands Instituut Fysieke Veiligheid)
Prof. dr. Georg Frerks (Universiteit Wageningen)
Prof. dr. Bob de Graaff (Nederlandse Defensie Academie)
Prof. dr. Ira Helsloot (Radboud Universiteit Nijmegen)
Prof. dr. Erwin Muller (Universiteit Leiden)
Dr. Astrid Scholtens (Crisislab)
Prof. dr. Erwin Seydel (Universiteit Twente)
Prof. dr. Rob de Wijk (The Hague Centre for Strategic Studies)

Aan dit nummer werkten mee:
Marjolein van Asselt, Edwin Bakker, Bianca Beck, Marcel van Berlo, Esther van Beurden, Jan Bos, Mathilda Buijtendijk, Ronald Christiaans, Ivonne Couwenberg, Sabine Geerdes, Désirée Geerts, Barbara Geurtsen, Leatitia Griffith, Jolanda de Haas, Johan van Hall, Hanneke Heeres, Ira Helsloot, Jorien Holsappel, Katinka van der Hooft, Ben Janssen, Nikki Jansweijer, Rob Jastrzebski, Wouter Jong, Carlo Kahn, José Kerstholt, Friso Meijer, Erwin Muller, Andrea Naphegyi, Ruud Oord, Margo van Ostaijen, Jan Wolter Ouwehand, Barry van 't Padje, Elte Palm, Johan Peekstok, Els Poeder, Astrid Scholtens, Gonne Schras, Marloes Smelter, Mirjam Snoerwang, Marijke Stokkel, Léon Strous, Petra Timmers, Gijs Tra, Maaike van Tuyll, Arjan Uilenreef, Willem Vermeend, Esther Versluis, Vincent van der Vlies, Daan Weggemans, Hans van Zon

Fotografie
ABN AMRO, Crisisplein, Falck, Gezamenlijke Brandweer, Maarten Hilbrandie, Ruud Jansen, Nederlandse Veiligheids-branche, NCTV, NIBHV, Schiphol, Eric Sijtsma, Waterschap Noorderzijlvest

Illustraties
ABN AMRO, Burgernet, Danish Emergency Management Board, Gezamenlijke Brandweer, NATO

Cartoon
Arend van Dam

Vormgeving
Grafisch Buro van Erkelens, Den Haag

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

Druk
DamenVanDeventer

ISSN 1875-7561

Voor een gratis abonnement mail: crisisbeheersing@minbzk.nl.

Het magazine is te downloaden via www.rijksoverheid.nl/onderwerpen/crisis-en-nationale-veiligheid.

Vier vragen aan:

Willem Vermeend,
o.a. internet ondernemer, bestuurder, hoogleraar, auteur, oud-staatssecretaris en oud-minister over publiek private samenwerking (PPS)

Wat is volgens u publiek private samenwerking in de kern?
"PPS komt er op neer dat je een opdrachtnemer niet laat inschrijven op een vast omschreven uitvraag waarbij de laagste inschrijver de opdracht krijgt, maar formuleert welke output je als opdrachtgever gerealiseerd wilt hebben. Daardoor kan de potentiële opdrachtnemer veel meer eigen creativiteit inzetten. Het risico voor de opdrachtgever wordt veel lager, de kosten zijn overzichtelijker en de mate van voorfinanciering is veel geringer of zelfs helemaal niet meer nodig.
Als opdrachtgever moet je wel durven 'loslaten' en niet-kerntaken durven overdragen aan partijen die daar simpelweg beter in zijn. Dat eist absoluut visie, omdat iedereen gedwongen wordt tijdsbestendige en robuuste oplossingen te bedenken. Deze impliciet 'gedwongen discipline' zorgt er in de praktijk voor dat PPS contracten zoveel meerwaarde opleveren."

Hoe doet Nederland het op dit terrein in vergelijking met andere landen, hoe komt dat en zijn er landen waar we van kunnen leren?
"Nederland is lange tijd een achterblijver geweest, vooral als gevolg van de tot voor kort goede financiële positie van ons land. Overheden beschikten veelal over voldoende eigen middelen om zonder samenwerking met private partijen bepaalde projecten uit te voeren. Bovendien waren de betrokken ambtenaren gehecht aan bestaande en gebruikelijke (aanbestedings)procedures. Dat slimme PPS-en tot wel 20% meerwaarde kunnen opleveren, was minder relevant want het geld lag toch al klaar op de plank. In verschillende andere landen zoals Engeland, Duitsland, Frankrijk en België is PPS wel van de grond gekomen. De voorbeelden en ervaringen uit die landen zijn in het algemeen positief en daaruit kunnen wij lering trekken. Maar we kunnen ook leren van de missers die her en der onmiskenbaar zijn gemaakt. Bij PPS Netwerk Nederland, waar ik voorzitter van ben, zien we inmiddels een sterk toegenomen vraag naar praktijkvoorbeelden. We hebben een gratis quick scan ontwikkeld waarmee snel kan worden vastgesteld waar vooral wel maar ook niet PPS kansen liggen."

Het PPS Netwerk Nederland heeft een focus op andere domeinen dan veiligheid. Hoe kijkt u echter aan tegen publiek private samenwerking op het gebied van nationale veiligheid en crisisbeheersing?
"PPS heeft ook te maken met de mindset: wil ik andere partijen mijn niet-kerntaken laten uitvoeren, kan ik voldoende lange termijn zekerheid en vertrouwen krijgen, stel ik mij zo open maar ook zelfbewust op dat ik mijn mogelijke leveranciers wat dieper in mijn visie e.d. wil laten kijken zodat ze kunnen meedenken, weet ik intern wat ik wil met mijn huidige organisatie, enz.? Het zou niet al te veel zou moeten uitmaken of je je gebouw wilt laten bouwen en runnen of diensten op gebied van veiligheid e.d. wilt laten verrichten. De Kromhout Kazerne in Utrecht is een mooi voorbeeld maar denk ook aan logistieke-, IT- en beveiligingsdiensten. Gevangenissen worden reeds in PPS gebouwd, dus je ziet dat daar waar opdrachtgevers vroeger ervan overtuigd waren dat 'alles' door de eigen dienst moest worden gedaan, voor volledig eigen rekening en risico ook op terreinen waar anderen simpelweg op meer ervaring en kennis kunnen bogen, er nu meer en meer daadwerkelijk wordt losgelaten. Resultaat is dat er tegen minder geld, meer kwaliteit wordt gemobiliseerd."

Bij PPS heeft iedereen zijn eigen verantwoordelijkheid en lopen de belangen soms uiteen. Wat is in die situaties de sleutel tot succes?
"Het gaat vooral om positief te denken in de zin van kansen. 'Waar en hoe zou een PPS eventueel kunnen' en niet meteen gaan focussen waarom het niet zou kunnen. PPS is geen wondermiddel dus het beter begrijpen waar PPS wel zinvol is of niet is, is ook belangrijk. Daag private partijen uit door ze met je probleem te confronteren en ze om een oplossing te vragen. Vertrouwen in de ander kun je wederzijds creëren door samen van gedachten te wisselen en vast te stellen wat je wel of niet voor elkaar kunt betekenen. Als het goed is, lopen bij een PPS de belangen juist niet uiteen maar worden er doelstellingen, serviceniveaus, enzovoorts geformuleerd waarbij beide partijen – de opdrachtnemer via bijvoorbeeld een variabele beloning- belang hebben om deze de doelen ook daadwerkelijk gerealiseerd te krijgen. Het niet benutten van PPS potentie daar waar deze er wel is, betekent het missen van voordelen op operationeel en financieel vlak. Ook een mogelijke kwaliteitsverbetering loop je mis. In het verleden was er bij overheden weinig animo. In de huidige situatie met aanzienlijke bezuinigingen zien we een kentering: de voor- en nadelen van PPS komen nu wel ter tafel."