



Nationaal Coördinator  
Terrorismebestrijding en Veiligheid  
Ministerie van Veiligheid en Justitie

jaargang 11 | nummer 1 | februari 2013

Magazine

# ationale veiligheid en crisisbeheersing

*Thema: Innovatie en R&D*

*Asbestvondst Kanaleiland: over evalueren en oordelen*

*Onzekere toekomsten in de Nationale Risicobeoordeling*

*Tien verbetervoorstellen voor crisisbeheersing*



# Inhoud

## THEMA: INNOVATIE EN R&D

**3** | Innovatie en R&D – een inleiding (prof. Sandro Etalle) **6** | Innovatie in de wereld van veiligheid en justitie **8** | Nederland Veilig door Innovatie **9** | Nationale veiligheid via internationale samenwerking **10** | Maakt het Topsectorenbeleid Nederland rijker en veiliger? **11** | “Veiligheid schreeuwt om innovatie” **12** | Hoe de ‘wisdom of crowds’ kan bijdragen aan veiligheid **14** | The Hague Security Delta ontwikkelt campus voor innovatie en veiligheid **15** | Hou veiligheid in de gaten – inkoopinnovatie urgent **16** | Defensie en innovatie **18** | Internetgedreven innoveren vergroot veiligheid **19** | Succesvolle innovatie vereist diversiteit en continuïteit! **20** | Open innovatie in een gesloten omgeving **22** | Bedreigingen via internet **23** | Digitaal bewijs onder de motorkap **24** | Hoe en waarom je innoveert is belangrijker dan wat je innoveert **56** | Vier vragen aan: Leo Zaal, algemeen directeur Instituut Fysieke Veiligheid

## OVERIGE ONDERWERPEN

**26** | Onzekere toekomsten in de Nationale Risicobeoordeling **28** | Commissie Onderzoek asbestvondst Kanaleneiland **30** | De asbestcrisis in Utrecht: over evalueren en oordelen **34** | De beoordelaars beoordeeld! **35** | Leren van de asbestcrisis **36** | Crisisbeheersing naar een substantieel hoger niveau **39** | “Communicatie moet bestuurders coachen bij crises” **40** | Slachtoffer Informatie Systematiek **43** | Aandacht voor risico’s digitaal verkeer door campagne Alert Online **44** | Rechtvaardige selectie van patiënten bij een pandemie **46** | GROTER – Oranje kolom uit de startblokken **48** | De rol van slachtoffers binnen de context van contraterrorisme **50** | Superstorm Sandy – getrokken lessen en een Nederlandse aanpak in New York City **52** | Afwegingsinstrument Veiligheid en Economie **54** | Gaan sociale media 1-1-2 vervangen?

Het Magazine nationale veiligheid en crisisbeheersing is een tweemaandelijks uitgave van de Nationaal Coördinator Terrorismebestrijding 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 uitgever is het niet noodzakelijkerwijs eens met de inhoud van gepubliceerde bijdragen. De verantwoordelijkheid en aansprakelijkheid voor de inhoud van de artikelen berust bij de auteurs.



prof. dr. Sandro Etalle,  
hoogleraar Embedded System  
Security, Technische Universiteit  
Eindhoven (en tevens Universiteit  
Twente)

# Innovatie en R&D

## - een inleiding

De redactiecommissie heeft mij verzocht een bijdrage te schrijven ter inleiding van het onderwerp Innovatie. Toen ik de uitnodiging aannam, realiseerde ik me dat ik hooguit mijn persoonlijke - dus vooringenomen - visie kon geven. Ik hoop dat de lezers me dat niet kwalijk nemen. Veiligheid is een buitengewoon ruim begrip: het is dan ook geen wonder dat het niet met één woord in het Engels vertaald kan worden. Veiligheid omvat namelijk zowel *safety* als *security*. De meeste lezers zullen doordrongen zijn van het verschil. Preventie en management van incidenten, zoals overstromingen, zijn een kwestie van *safety*, maar in het geval van bewuste aanvallen (bijvoorbeeld spionage) komen we op het terrein van *security*.

In dit artikel beperk ik me tot *security*.

Dat is overigens niet omdat er voor *safety* geen R&D nodig zou zijn; verre van zelfs. Denk bijvoorbeeld aan de geweldige resultaten die de afgelopen decennia konden worden geboekt om de *safety* te verbeteren. Een goed voorbeeld daarvan zijn de simulatietechnieken. Die zijn enorm vooruitgegaan en dragen nog steeds bij aan de verbetering van de veiligheid van de luchtvaart. Opgemerkt mag worden dat - wederom dankzij belangrijke stappen op R&D-gebied - hetzelfde concept nu toegepast gaat worden op het terrein van *serious gaming*, zodat mensen bijvoorbeeld veilig kunnen trainen en oefenen ter voorbereiding op interventies in gevaarlijke gebieden. Natuurlijk zijn simulatietechnieken slechts een van de vele verbeteringen via R&D die ons dagelijks leven veiliger hebben gemaakt.

In het geval van *security* krijgen we te maken met een nieuwe factor: de tegenstander. Een dief, een crimineel, een cyberterrorist, een maffiabaas en ga zo maar door. Vanwege deze tegenstanders, met hun eigen belangen en soms zelfs hun eigen R&D-activiteiten, is *security* in het algemeen en cyber *security* in het bijzonder, een terrein geworden met enorme uitdagingen die we alleen het hoofd kunnen bieden met een combinatie van alertheid, intelligent ingezette informatie, doordacht beleid en hoogwaardige R&D.

Wat betreft cyber *security* is de wereld volstrekt niet meer te vergelijken met wat ze ooit was. Wij, de burgers, hebben ons helaas weliswaar nooit helemaal veilig gevoeld bij het gebruik van computers en geautomatiseerde systemen, maar tot voor kort wisten we onze gegevens over het algemeen veilig te stellen. Nu bevinden onze gegevens zich overal en zijn ze permanent beschikbaar, bovendien hebben we ze meestal niet in eigen hand. Een aanval waarbij je thuis via je iPhone een normaal uitzijnde e-mail opent, kan ertoe leiden dat de veiligheid van je netwerkrouter gecompromitteerd raakt.<sup>1</sup> Zoiets was een paar jaar geleden nog ondenkbaar: destijds had je nog geen smartphone en wellicht ook geen router. Hetzelfde gaat op voor onze vitale infrastructuur, die jarenlang met rust gelaten werd, maar volgens het Amerikaanse Department of Homeland Security een relatief eenvoudig doelwit is geworden voor hackers. Amerikaanse industriële systemen werden in 2012 vaker dan ooit getroffen door aanvallen. Er werden toen bijna 200 van dit soort incidenten gemeld.<sup>2</sup> We hebben allemaal gezien hoe de aanvallen zich ontwikkeld hebben. Tot een paar jaren geleden waren ze nog hoofdzakelijk afkomstig van amateurs, maar al spoedig werden ze professioneler, toen de eerste *banking malware* en identiteitsfraude zich aandienen (nu kon er ook geld mee verdiend worden).

<sup>1</sup> <http://www.acunetix.com/blog/web-security-zone/the-email-that-hacks-you/>

<sup>2</sup> <http://www.eweek.com/security/industrial-control-systems-faced-nearly-200-attacks-dhs/>



Sinds 2009-2010 hebben Stuxnet, Duqu, Shamoon, Flame en Gauss er een nieuwe dimensie aan toegevoegd: het kost miljoenen om dergelijke malware te ontwikkelen, die in sommige gevallen is gebruikt voor slechts een single target. Dit zijn de zogenaamde targeted attacks. Ze zijn buitengewoon geavanceerd en duur, maar kosten nog altijd minder dan een raket (denk ook aan Frankrijk dat de VS beschuldigde van het gebruik van malware om het Élysée te bespioneren<sup>3</sup>. Volgens een Visiongain Report zal er op de wereldmarkt voor cyberoorlogsvoering in 2013 zo'n US\$ 16.96 miljard omgaan.<sup>4</sup>

Ondertussen voltrekken zich ingrijpende wijzigingen in bepaalde economische mechanismen achter cyber security. Voor de good guys in de cyberveiligheid viel er natuurlijk nooit veel te verdienen. Tot een paar geleden loonde een carrière als bad guy echter ook niet bepaald, óf je moest bereid zijn nauw samen te werken met criminelen. Met name op dit punt is er de afgelopen paar jaar echter veel veranderd. Dankzij de groeiende markt van tussenpersonen is het voor hackers namelijk lucratief en eenvoudig geworden een slaatje te slaan uit

de kwetsbaarheden van systemen.<sup>5</sup> Naar verluidt is er onlangs maar liefst US\$ 250.000 neergeteld voor een kwetsbaar punt, wat beslist meer is dan een hacker zou kunnen verdienen door het te melden bij de legitieme verkoper.<sup>6</sup> Zero Day van Tipping Point is dan ook een lovenswaardig initiatief (het belonen van bonafide hackers) dat hopelijk veel navolging zal krijgen.

Dus, wat moeten we nu alles met alles samenhangt, onze gegevens rondzweven in clouds, onze vitale infrastructuur kwetsbaar is, de economische mechanismen in het voordeel werken van de bad guys en we het vooral moeten doen met nationale middelen om de internationale cybercriminaliteit het hoofd te bieden? Mijn voorstellen stroken grotendeels met hetgeen reeds gedaan is en komen neer op drie punten: (a) raak niet in paniek, (b) investeer in degelijk beleid dat niet beïnvloed is door lobbyisten en een goede balans vormt tussen privacy, security en accountability, en – last maar absoluut niet least – (c) investeer in R&D.

De regio Eindhoven met Philips, ASML en al hun spin-offs vormt het levende bewijs dat R&D niet alleen leidt tot verbetering van de kwaliteit van het leven, maar ook economisch rendeert. Brainport Regio Eindhoven helpt ideeën te vertalen in waarde door de samenwerking tussen bedrijfsleven, onderzoek en overheid te stimuleren. Zo ontstaat er een klimaat dat bevorderlijk is voor hightech business.

En R&D voor security leidt niet alleen tot een beter begrip van de risico's die ons boven het hoofd hangen en betere manieren om ze aan te pakken, maar levert ook economisch rendement op. Het is geen toeval dat het stimuleren van de Nederlandse security-economie als een van de vier doelen prijkt op de National Cyber Security Research Agenda.<sup>7</sup> Het initiatief voor deze agenda, die omarmd wordt door het NCSC is oorspronkelijk afkomstig van het ICT-innovatieplatform Veilig Verbonden. De overige drie doelen zijn: verbetering van de security en betrouwbaarheid van de ICT-infrastructuur, voorbereiding op de security-uitdagingen in Nederland voor de komende tien tot twintig jaar en versterking en verbreding van het Nederlandse security-onderzoek door bevordering van samenwerking.

<sup>3</sup> <http://www.techspot.com/news/50880-us-blamed-for-spying-on-french-government-with-flame-malware.html>

<sup>4</sup> <http://www.air-cosmos.com/news/pr-newswire/global-cyber-warfare-market-to-be-worth-16-96bn-in-2013-says-visiongain-report.html>

<sup>5</sup> <http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/>

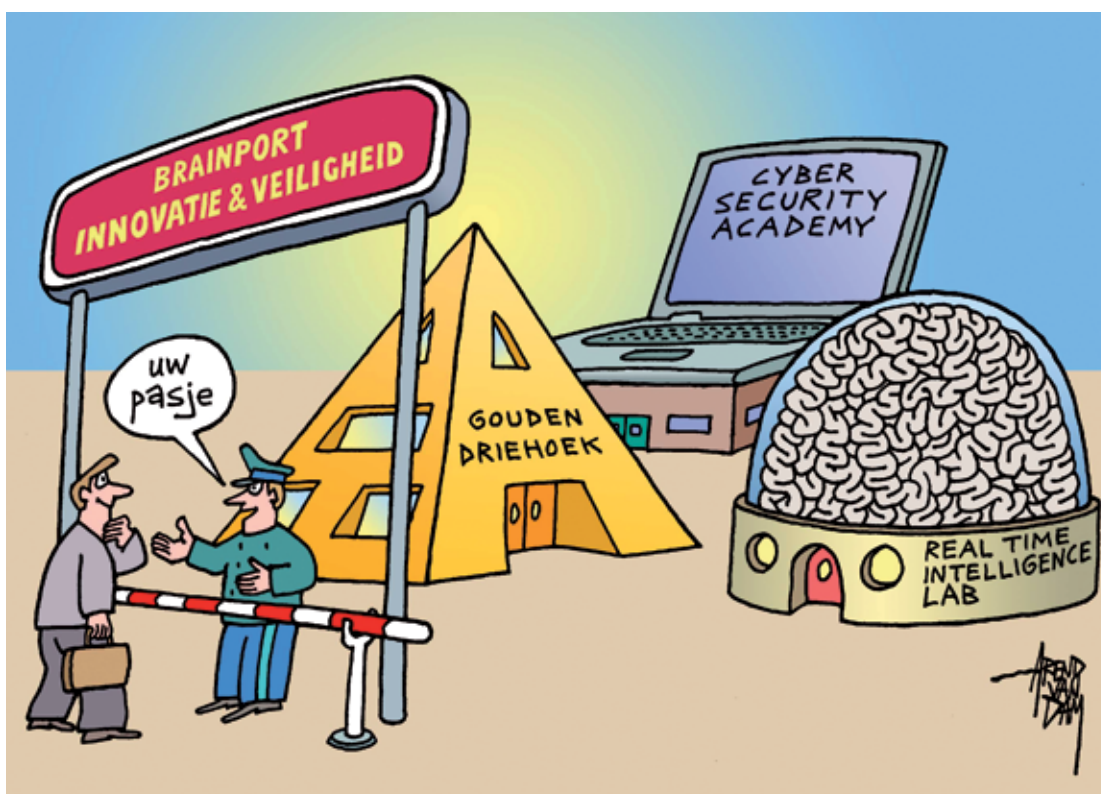
<sup>6</sup> [http://www.schneier.com/blog/archives/2012/04/buying\\_exploits.html](http://www.schneier.com/blog/archives/2012/04/buying_exploits.html)

<sup>7</sup> CSRA, [http://www.nwo.nl/files.nsf/pages/NWOP\\_8VTGRM\\_Eng/\\$file/Cyber%20Agenda.pdf](http://www.nwo.nl/files.nsf/pages/NWOP_8VTGRM_Eng/$file/Cyber%20Agenda.pdf)

Als een goed voorbeeld van hoe R&D op het gebied van security goede resultaten, betere security en waarschijnlijk iets moois voor de Nederlandse economie kan opleveren, wil ik de projecten Hermes-Castor-Midas noemen, die specifiek gericht zijn op de bescherming van de vitale infrastructuur. Om de focus van het project te waarborgen, zijn we begonnen met een consortium van niet alleen kennisorganisaties (in dit geval de groepen DIES en DACS van de Universiteit Twente), maar ook eindgebruikers (ABB, Waternet, Alliander, Gasunie, Brabant Water) die probleemeigenaar waren en twee aanbieders van oplossingen (FoX-IT, en de 3TU spin-off SecurityMatters) die de onderzoeksresultaten zo nodig in levensvatbare oplossingen zouden kunnen vertalen. In 2008-2009 (dus vóór Stuxnet) begonnen we met de vraag hoe onze expertise te gelde te maken om de vitale infrastructuur van nutsbedrijven te beschermen. We hebben onze ideeën gepresenteerd aan de partners, een consortium gevormd en vervolgens een projectvoorstel ingediend bij het ministerie van Binnenlandse Zaken dat later door zijn opvolger, het ministerie van Veiligheid en Justitie, werd aangenomen. Een jaar later werd Stuxnet ontdekt (we hadden geluk). De lezer herinnert het zich waarschijnlijk nog: Stuxnet was zo ontworpen dat het vrijwel ondetecteerbaar zou zijn voor security-oplossingen. Naderhand bleek echter dat een aantal van de ideeën waarmee we bezig waren, geschikt waren om zonder aanpassingen Stuxnet te

detecteren. Dat was dus niet alleen een kwestie van geluk. Nu, een paar jaar later, omvatten de resultaten van dit project, afgezien van papers, presentaties op wetenschappelijke conferenties, nieuwe EU-projecten in samenwerking met internationale partners en deelname in een professionele organisatie, met name ook nieuwe bruikbare technologie. Bepaalde resultaten van HCM zullen wellicht nooit verder komen dan de tekentafel, maar andere maken reeds deel uit van zeer innovatieve systemen voor netwerkmonitoring die het landschap van de netwerkverdediging de komende jaren naar alle waarschijnlijkheid ingrijpend zullen veranderen en direct zelfs de meest geavanceerde bedreigingen voor netwerken zullen oppikken.

Natuurlijk levert niet alle security-onderzoek verbeteringen op en/of een leuk rendement. Maar zo moet het ook, want als je de onvoorspelbaarheid eruit haalt, krijg je alleen voorspelbare resultaten, en dat is nu net niet waar het bij highrisk-highreturn onderzoek om draait. Hermes-Castor-Midas vormt een fantastische combinatie van onderzoekers met briljante ideeën, een ontvankelijke markt en tot op zekere hoogte een portie geluk in de vorm van goede timing. Bepaalde factoren kunnen niet volledig gecontroleerd worden, maar wel worden gefaciliteerd door slimme connecties tussen onderzoekers, mensen uit de praktijk en probleemeigenaren.





# Innovatie in de wereld van veiligheid en justitie

Het Amerikaanse bedrijf Innocentive brengt oplossters (*solvers*) en partijen met een vraag (*seekers*) bij elkaar. Begonnen als een plek waar farmaceuten onopgeloste laboratoriumvraagstukken konden posten, zijn inmiddels bijna 300.000 *solvers* uit meer dan 200 landen aangesloten die een enorm spectrum van vraagstukken helpen oplossen. [www.innocentive.com](http://www.innocentive.com) is wat men noemt een 'open innovatieplatform' – een plek waar organisaties kunnen putten uit het enorme potentieel aan kennis en kunde dat buiten hun eigen organisatiegrenzen aanwezig is. Innocentive is daarmee ook een bron van inspiratie voor alle vernieuwers in de wereld van veiligheid en justitie waar we ook kunnen verwachten dat veel nieuwe mogelijkheden om sneller, slimmer en effectiever te werken van buiten zullen komen.

**Krijn van Beek,**  
directeur Strategie en  
voorzitter R&D-council,  
Ministerie van Veiligheid  
en Justitie

Om innovatie in ons domein een extra impuls te geven, is najaar 2012 een Council voor R&D en Innovatie ingesteld binnen het ministerie van VenJ. De council is adviseur van de bestuursraad. In het navolgende zal ik kort aangeven waarom innovatie binnen het VenJ-domein extra impulsen nodig heeft, waarom dit juist in dit domein ingewikkeld is en wat de council van zins is te gaan doen.

## Definitie van innovatie

De 'Oslo Manual' van de OECD definieert innovatie als: de implementatie van een nieuw of wezenlijk verbeterd product/dienst/proces. Omdat niet elke vernieuwing per se een verbetering is, kunnen we hieraan voor de publieke sector toevoegen (vgl. de innovatiemonitor van InAxis) dat een innovatie vereist: een merkbaar effect in termen van doeltreffendheid en/of doelmatigheid.

Innovatie gaat dus niet alleen over techniek, maar vooral ook om logistiek, organisatie, productie, samenwerking, benutting, etc. Een innovatie hoeft ook niet nieuw te zijn uitgedacht, nieuw voor de organisatie is goed genoeg, nieuwe combinaties is goed genoeg. Ten slotte geeft de definitie aan dat een innovatie pas een innovatie is als die ook daadwerkelijk wordt toegepast: een uitvinding blijft een uitvinding ook als die nooit het laboratorium verlaat, een innovatie telt alleen als die daadwerkelijk op de werkvloer wordt ingezet.

## Innoveren in veiligheid én recht

Als we innoveren in veiligheid dan raakt dat bijna automatisch ook het recht. En andersom: innovaties in het recht zijn bijna automatisch ook innovaties in veiligheid. Vaak wordt er gesproken in termen van een afruil

tussen deze twee, maar dat is niet waar de innovatie zich op richt. Bijvoorbeeld privacy inleveren voor het bestrijden van terrorisme. Dat is een keuze, maar de innovatie-uitdaging zou zijn om terrorisme te bestrijden zonder privacy in te leveren. In de economie heet zo iets het streven naar een Pareto-verbetering: je wilt verbetering op tenminste één dimensie zonder verlies te lijden op enige andere dimensie. Pareto-verbeteringen, dat is waar we naar streven en daarom is het belangrijk om innovaties in het domein van veiligheid en recht als één geheel te beschouwen.

### Urgentie van innovatie in veiligheid en recht

Nederland is de afgelopen jaren veiliger geworden. Tenminste de dreiging van terroristische aanslagen is gedaald, het aantal slachtoffers van moord en doodslag is gedaald, de *high impact crime* loopt terug en nog zo wat indicatoren die de goede kant op bewegen. Tegelijk stelt de samenleving voortdurend hogere eisen, zowel op het gebied van veiligheid als op het gebied van recht. Het regeerakkoord van het kabinet Rutte-Asscher noemt een indrukwekkende set ambities die stuk voor stuk serieuze innovatie vereisen. Het regeerakkoord noemt bijvoorbeeld: toename van de veiligheid, toename van de pakkans, terugdringen recidive, verbetering van de positie van het slachtoffer, bescherming van de persoonlijke levenssfeer, eerbiediging van de persoonlijke levenssfeer, doelmatiger strafrechtsketen, verkorting van doorlooptijden van strafzaken, het civiele proces wordt vérgaand vereenvoudigd en gedigitaliseerd. Deze ambities staan echter onder het gesternte van afnemende middelen, wat innovatie nog urgenter maakt.

Voor de wat langere termijn worden de uitdagingen alleen maar groter. Technologische ontwikkeling, grensoverschrijdend verkeer en veranderende maatschappelijke verhoudingen zullen de komende jaren allerlei nieuwe vragen oproepen en tegelijk allerlei nieuwe mogelijkheden gaan bieden. Deze ontwikkelingen maken innovatie eens te meer urgent. Tegelijk is innovatie in het domein van veiligheid en recht extra ingewikkeld. De rechtsstaat is bij uitstek het domein van continuïteit en van voorspelbaarheid; innovatie lijkt daar haaks op te staan. Veiligheid is bij uitstek een domein dat de overheid zelf doet, gegeven haar geweldsmonopolie – daar waar het voorbeeld van Innocentive aangeeft hoezeer we kunnen profiteren als we actief de openheid zoeken om onze uitdagingen te etaleren en samen met de gemeenschap die we dienen op zoek gaan naar oplossingen. Dat zijn twee fundamentele spanningen die bijzondere aandacht voor innovatie in ons domein noodzakelijk maken.

### De impulsen van de council

Als we met de hiervoor genoemde uitdagingen de

komende jaren verder willen komen in veiligheid én recht, zullen we goed moeten worden in het betrekken van oplosers bij de vraagstukken waar we voor staan. Die oplosers zullen zich vaak buiten het VenJ-domein bevinden en we hebben hun kennis nodig en hun netwerken en slimme gezamenlijke inzet.

De huidige praktijk laat al een aantal succesvolle voorbeelden zien: veiligheidshuizen (samenwerken met lokale partners), winkeldiefstal (samenwerken met winkeliers), nationale veiligheidsstrategie (samenwerken met vitale infrastructuurbeheerders), cyber security (samenwerken met internet providers, misschien zelfs met hackers), internetconsultatie (wetgevers die open samenwerken met deskundigen van buiten). Deze manier van werken zal de komende jaren verder uitgebouwd moeten worden om de kernwaarden van recht en veiligheid te kunnen dienen in een omgeving die meer en andersoortige eisen stelt.

Daarin schuilt precies de opdracht van de pas opgerichte R&D-council van VenJ. De council telt leden uit de belangrijkste geledingen van het ministerie die vanwege hun visie op innovatie op persoonlijke titel in de council zijn benoemd. De council adviseert de bestuursraad en gaat ervan uit dat innovatie in belangrijke mate een *bottom up* fenomeen is, dat echter wel een aantal centrale impulsen nodig heeft. Op dit moment zijn we in nauw overleg met de departementsleiding bezig met het vormgeven van de rol van de council en denken we aan twee soorten impulsen: richting geven en markt organiseren.

Richting geven kan de council door in nauw overleg met de beleidsdirecties een handvol grote uitdagingen te formuleren: in het verlengde van de huidige beleidsdoelen maar een ordegrootte verder. Deze richtinggevende uitdagingen moeten als een soort magneet werken op innoverende mogelijkheden binnen en buiten het departement.

Om te zorgen dat partijen elkaar ook daadwerkelijk kunnen vinden, kan de council marktplaatsen organiseren. In de inleiding werd al gewezen op Innocentive als een voorbeeld van zo'n marktplaats waar vragers en aanbieders elkaar treffen. Je zou ook aanbieders onderling bij elkaar kunnen brengen zodat ze functionele consortia kunnen vormen. Naast Innocentive zien we meer inspirerende voorbeelden van dergelijke marktplaatsen: [www.slimmernetwerk.nl](http://www.slimmernetwerk.nl) bijvoorbeeld is een initiatief van het ministerie van BZK. [www.innovatingjustice.org](http://www.innovatingjustice.org) is een initiatief van The Hague Institute for the Internationalisation of Law (HIIL) om wereldwijd justitie-innovaties te inventariseren.

Geheel in lijn met het voorgaande zijn suggesties en ideeën voor de werkzaamheden van de council zeer welkom.

**But Klaasen,**  
innovatiemanager NCTV  
**Edmée Moojen,**  
adviseur Innovatie NCTV  
**Stéphanie de Vroet,**  
deelprojectleider Innovatie NCTV

# Nederland Veilig door Innovatie

Nederland moet veilig zijn, veilig blijven en Nederlanders moeten zich veilig voelen. De wereld om ons heen verandert snel en het bijhouden van de nieuwe (technologische) ontwikkelingen is een uitdaging. Voor de operationele partners in het veiligheidsdomein is het echter van levensbelang om snel in te kunnen spelen en gebruik te maken van de nieuwste kennis, inzichten en ideeën.

Het Ministerie van Veiligheid en Justitie (VenJ) ziet kennis en innovatie daarom als een noodzaak om onze maatschappij veiliger te maken. Wij moeten ons werk steeds slimmer, effectiever en efficiënter doen. Maar hoe stimuleert het Ministerie de ontwikkeling van innovatieve kennis én toepassingen op het gebied van maatschappelijke veiligheid?

## Programma Veilig door Innovatie

Sinds 1 oktober 2012 is de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) binnen het Ministerie verantwoordelijk voor het programma 'Veilig door Innovatie'. Vanuit dit programma wil VenJ innovatieve kennis en toepassingen stimuleren, het liefst met ideeën van buitenaf. Publieke veiligheidsorganisaties kunnen een financiële stimulans krijgen voor innovatieve projecten die de maatschappelijke veiligheid ten goede komen. Hierbij moet u niet alleen denken aan *state of the art* technologie maar juist ook aan

sociale en organisatorische (aspecten van) innovaties. Zo zijn er in het verleden projecten gedaan op het gebied van (alternatieven voor) brandbestrijding; de mogelijkheden van *datamining* en analysetools op het internet (social media); de betrokkenheid van burgers bij het oplossen van veiligheidsvraagstukken; en de mogelijkheden van de inzet van camera's in het publieke domein. Zie ook het voorbeeld van de CrashCube van Rotterdam-Rijnmond.

## Samenwerken in de 'Gouden Driehoek'

De publieke veiligheidspartners in Nederland staan voor grote uitdagingen. Dit kunnen zij niet alleen. De beste ideeën en oplossingen ontstaan vaak uit een combinatie van expertises. Zoals u in de volgende pagina's kunt lezen, zijn zowel private als publieke partijen in Nederland sterk in het vergaren van de nieuwste kennis, inzichten en toepassingen om de maatschappelijke veiligheid te vergroten. Samen kunnen overheidspartijen, industrie

en kennisinstituten (de Gouden Driehoek) komen tot nieuwe en excellente uitkomsten voor veiligheidsvraagstukken. Een mooi voorbeeld hiervan kunt u lezen in het artikel van Roelof Muis over 'dreigtweets'. De activiteiten van NCTV op het domein van veiligheid en innovatie hangen uiteraard nauw samen met de recent opgerichte R&D Council van het ministerie. Voorzitter van de Council Krijn van Beek spreekt elders in dit blad dan ook terecht over "innoveren in veiligheid èn recht". Want op alle domeinen van het ministerie willen we innovatie stimuleren door het bieden van een ontmoetingsplaats voor de innovators uit de Gouden Driehoek (tijdens congres, symposia en andere themadagen). Zie het als een marktplaats voor innovatieve kennis en toepassingen waar vraag en aanbod elkaar vinden en waar ruimte wordt geboden aan experimenten, creativiteit en lef.

## Innovatie over de grenzen

Hoe beter wij de voedingsbodempoor innovatieve kennis en toepassingen op het gebied van veiligheid weten te organiseren, hoe beter wij deze voedingsbodempook vanuit andere landen kunnen voeden. Wij kunnen immers van anderen leren, en anderen van ons. VenJ ziet hiervoor een belangrijk (en groot) Research & Development instrument in de Europese Unie, wat nu het Zevende Kaderprogramma (KP7) is en vanaf het jaar 2014 "Horizon 2020". Meer hierover kunt u lezen in het artikel van Paul Kruis van Agentschap NL. Ook in Europa moeten de Nederlandse partijen uit de Gouden Driehoek de handen ineen slaan om met Europese partners nog meer kennis, inzichten en toepassingen te genereren om veiligheidsvraagstukken het hoofd te kunnen bieden. Niet alleen in Nederland maar ook in de rest van de Europese Unie.

Voor meer en de laatste informatie over het programma Veilig door Innovatie binnen het Ministerie van VenJ zie: [www.nctv.nl/innovatie](http://www.nctv.nl/innovatie).





# Nationale veiligheid via internationale samenwerking

De Europese Commissie stimuleert al jaren onderzoek en innovatie via een subsidieregeling die het Kaderprogramma (KP) wordt genoemd. Binnen de EU is dit Kaderprogramma het omvangrijkste programma voor onderzoek en heeft veruit de grootste budgetten. Via subsidies worden verschillende vormen van internationaal onderzoek gestimuleerd. Een programma dat zo succesvol is, dat we momenteel in het Zevende Kaderprogramma (KP7) zijn beland.



De Kaderprogramma's kennen verschillende onderzoeksthema's waarin internationale consortia samenwerken in vooruitstrevend onderzoek, zoals o.a. ICT, milieu of energie. In de eerste zes Kaderprogramma's stond veiligheid hooguit incidenteel op de onderzoeksagenda's van de verschillende thema's. Dat is met het Zevende Kaderprogramma veranderd. Na de grote aanslagen in de VS en de EU werd duidelijk dat we ons beter moeten voorbereiden op kwaadwillend handelen van individuen en terroristische organisaties. Dat gaat niet alleen door het inzetten van meer veiligheidspersoneel. Nieuwe oplossingen zijn nodig voor een beter optreden in de veiligheidssector. Na de publicatie van verschillende rapporten met aanbevelingen voor een onderzoeksprogramma is vanaf 2007 het civiele veiligheidsonderzoek een apart onderzoeks-thema geworden in KP7, met een eigen budget. Behalve het vergroten van de veiligheid is het versterken van de Europese veiligheidsindustrie een belangrijke doelstelling voor de Europese Commissie.

KP7 loopt van 2007 tot en met 2013, waarbij circa 1,4 miljard euro beschikbaar is voor veiligheidsonderzoek. Universiteiten, kennisinstellingen, industrie en eindgebruikers uit verschillende landen werken samen om nieuwe kennis en technologie in te kunnen zetten voor de bescherming van vitale infrastructuur, crisismanagement, grensbewaking en criminaliteitsbestrijding. Naar verwachting zullen in totaal zo'n 300 Europese projecten voor veiligheid via het Kaderprogramma worden gefinancierd.

Met het einde van KP7 in zicht, worden de voorbereidingen voor een nieuw Kaderprogramma gestart. Al vanaf 2011 worden consultaties uitgezet en studies verricht voor het vormgeven van een nieuw onderzoeksprogramma. Vanaf 2014 willen de Europese Commissie en de lidstaten het onderzoek laten verlopen in een nieuw kaderprogramma dat voor het eerst een grote naamsverandering kent: het Horizon 2020 programma (H2020). Belangrijke uitgangspunten zijn een vereenvoudiging van de regels, een opzet die uitgaat van

maatschappelijke vraagstukken en een betere doorstroom van onderzoeksresultaten naar producten.

Het thema veiligheid komt dan ook terug als maatschappelijke uitdaging in H2020. De aandacht wordt verbreed en verdiept. Naast de bestaande onderwerpen komt nu extra aandacht voor cyber security en standaardisatie. Een verdere afstemming met defensie en het betrekken van de sociale wetenschappen zijn verdere belangrijke aspecten in H2020. Voor eindgebruikers en ontwikkelaars van veiligheidsoplossingen zijn er volop kansen om in internationale samenwerking te werken aan nieuwe technologie en kennis. Goed nieuws is dat het onderzoek dichter op de markt komt te staan. Activiteiten die in Nederland al plaats vinden via SBIR programma's (Small Business Innovation Research), zullen vergelijkbare instrumenten op Europese schaal krijgen. Voor eindgebruikers wordt deelname daarmee interessanter, omdat onderzoek dichter bij de oplossing zal komen die ze zoeken.

Het Ministerie van Veiligheid en Justitie, het Ministerie van Economische Zaken en Agentschap NL zijn alle drie betrokken bij de ontwikkelingen voor veiligheid in H2020. In de loop van 2013 zal steeds beter bekend worden welk onderzoek vanaf 2014 voor subsidie in aanmerking komt en onder welke voorwaarden. Met name de budgetten en de regels voor deelname zijn momenteel onderwerp van discussie. Om op de hoogte te blijven van de laatste ontwikkelingen, kunt u altijd contact opnemen met Agentschap NL.

# Maakt het Topsectorenbeleid Nederland rijker en veiliger?

De in de titel opgenomen vraagstelling bevat de vooronderstelling dat door het kiezen van een nieuwe economische beleidsvariant een verbeterde maatschappelijke opbrengst gerealiseerd kan worden. Met andere woorden, het bedrijfsleven heeft het voor het zeggen (hoofduitgangspunt van het Topsectorenbeleid) waar in Nederland de gelden voor kennisontwikkeling aan worden uitgegeven, met als verwachte opbrengst dat Nederland rijker en, in relatie tot Nationale Veiligheid, veiliger wordt.

## De overheid in de rol als launching customer

Bovenstaande inleiding heb ik gekozen om het Topsectorenbeleid in het perspectief van nationale veiligheid en crisisbeheersing te kunnen duiden. Een belangrijk bezwaar dat bij dit beleid kan worden aangekend is dat de koppeling met voornamelijk maatschappelijke thema's zoals gezondheid, infrastructuur, milieu, onderwijs en veiligheid ondergeschikt lijkt te zijn gemaakt aan de keuze om "het bedrijfsleven" te laten bepalen waar ook de publieke gelden voor onderzoek en ontwikkeling aan besteed moeten worden. Dat wringt natuurlijk, en in de opstart van het Topsectorenbeleid is dan ook vanuit meerdere partijen, inclusief het bedrijfsleven, gepleit om de overheidsrol als vragende (markt) partij beter te borgen. Dit heeft er toe geleid dat het vorige Kabinet de aanbeveling van de Topsector High Tech Systemen & Materialen heeft overgenomen om 2,5 % van het daarvoor in aanmerking komende inkoopvolume van de overheid (ordegrootte € 53 miljard) innovatief aan te besteden. De 'dubbelrol' van de overheid als *launching customer* naast de rol van co-financier van onderzoek en ontwikkeling zou daarmee een belangrijke impuls

kunnen opleveren om het zogenaamde marktfalen in specifieke markten zoals de veiligheidsmarkt, te helpen opheffen.

## Van Maatschappelijke Innovatie Agenda Veiligheid naar Roadmap Security

Zoals kosten voor de baten gaan loopt kennisontwikkeling voor op kennistoepassing, dus er zal eerst geïnvesteerd moeten worden in het aanbrengen van focus en impact in de nationale onderzoeksinspanning op het gebied van veiligheid. Gezamenlijk is door het bedrijfsleven, de 'veiligheidsministeries' Defensie en Veiligheid en Justitie, de universiteiten en de kennisinstellingen de Roadmap Security<sup>1</sup> opgesteld, waarbij de in het recente verleden opgestelde Maatschappelijke Innovatie Agenda Veiligheid als uitgangspunt genomen is.

Deze roadmap kiest voor kennisconcentratie op de thema's cyber security, actieve en passieve sensoren en system of systems. De aandacht voor cyber is vandaag de dag evident, op het gebied van actieve sensoren (met name radar) bekleedt Nederland een wereldtoppositie en bij passieve sensoren is naast akoestische sensoren (gevectoriseerd geluid) de aandacht met name gericht op intelligente beeldverwerkende technieken ten behoeve van gedrag en intentieherkenning. Met deze keuze voor onderscheidende technologiegebieden worden andere gebieden niet uitgesloten, maar die zullen onder andere arrangementen verder tot ontwikkeling moeten komen.

## Grootste innovatie uitdaging: netcentrisch verbinden van alle veiligheidspartners

Kortheidshalve kan gesteld worden dat de Roadmap Security de meest urgente technologie vraag en onze bestaande internationaal onderscheidende kennispositie combineert. Daarbij is *system of systems* zowel nationaal als internationaal een nieuw onderwerp

<sup>1</sup> <http://www.htsm.nl/Innovatie/Roadmaps>

waarbij de ambitie ligt op het verbeteren van het situatiebeeld in crisissituaties. Daarbij worden de verschillende informatieposities van alle relevante veiligheidspartners (inclusief de via social media aangesloten burger) operationeel gecombineerd tot een totaalbeeld waarop hyper dynamische besluitvorming, commandovoering en opvolging daadwerkelijk verbeteren. Netcentrisch samenwerken door alle bestuurslagen en publiek private verbanden heen, met en voor de burger en zo nodig grensoverschrijdend *real time* gecoördineerd. Deze activiteit bouwt voort op de volgende kenmerken van de Nederlandse economie en samenleving: een uitstekende ICT kennis positie en een zeer hoge economisch en sociaal toegepaste ICT dichtheid. Van grote waarde daarbij is bovendien dat met de system of systems ambitie goede aansluiting gevonden kan worden met de leidende thema's in Horizon 2020 van de Europese Unie.

**Grootste organisatorische uitdaging: verbinden van financiële middelen**

Ook een punt van zorg: system of systems vraagt om een systeemverantwoordelijke partij. Om op het juiste abstractieniveau de vraag te articuleren, gezamenlijke implementatieprojecten te definiëren, en tot afspraken te komen wie waarvoor betaalt. En dat laatste is mogelijk wel de grootste innovatie uitdaging op het

gebied van veiligheid. Om met Minister Plasterk te spreken: Nederland kent geen drie maar zes bestuurslagen, naast de lagen op Europees en nationaal niveau zijn er nog bestuurslagen op provincie, gemeente en deelgemeente niveau, en tenslotte het bestuur van de Waterschappen. Voeg daaraan toe de horizontale coördinatie op iedere bestuurslaag en de coördinatie met private partijen op alle niveaus, en het is duidelijk dat de operationele verantwoordelijkheid zo laag mogelijk belegd moet worden, maar de wetgeving en investeringsverantwoordelijkheid zo hoog mogelijk. Een voorbeeld daarvan is het verstrekken van evenementen vergunningen, waarbij er landelijk geen eenduidigheid bestaat over de kwaliteitseisen waaraan een evenementenorganisatie moet voldoen om de veiligheid van de bezoekers te waarborgen. Waardoor bij elk evenement het wiel opnieuw wordt uitgevonden en de beveiligers elkaar beconcurreren op prijs in plaats van het tegen de beste prijs leveren van de slimste en meest efficiënte veiligheidsoplossing passend bij het specifieke risicoprofiel van het evenement. De vraag is dus niet of we moeten investeren in veiligheid en innovatie, maar veel meer is de vraag te stellen wie in Nederland, in de context van het oppergezag en de kerntaak van de overheid op het gebied van veiligheid, en verwijzend naar de aanbeveling in het WRR-rapport *Evenwichtskunst*<sup>2</sup>, de systeemverantwoordelijkheid neemt.

## “Veiligheid schreeuwt om innovatie”

Op 10 december heeft Minister Opstelten uit handen van oud-directeur Nationale Veiligheid Henk Geveke het eerste exemplaar van de TNO-publicatie *Veiligheid schreeuwt om innovatie* in ontvangst genomen.



De publicatie is met steun van het NCTV programma 'Veilig door innovatie' tot stand gekomen en bevat een voorwoord van de minister en een interview met Erik Akerboom. Het boek beschrijft hoe met innoveren Nederland veiliger kan worden gemaakt. De minister benadrukte dat innovatie, juist in tijden van bezuinigingen, een goed instrument is om effectiever en goedkoper te gaan functioneren. De gehele publicatie is te downloaden via [www.tno.nl](http://www.tno.nl)

<sup>2</sup> [http://www.wrr.nl/fileadmin/nl/publicaties/PDF-overige\\_uitgaven/2011-12-06\\_\\_Evenwichtskunst\\_\\_volledige\\_publicatie.pdf](http://www.wrr.nl/fileadmin/nl/publicaties/PDF-overige_uitgaven/2011-12-06__Evenwichtskunst__volledige_publicatie.pdf)

# Hoe de 'wisdom of crowds' kan bijdragen aan veiligheid

Dankzij internet zijn we afgelopen decennia meer dan ooit verbonden geraakt. Het is nu beter mogelijk om wereldwijd informatie, ideeën en kennis uit te wisselen en samen te werken. Door dat slim te doen kunnen we gebruik maken van de zogenaamde 'wisdom of crowds': het feit dat we gezamenlijk betere beslissingen kunnen nemen en inschattingen kunnen maken dan individueel of dan alleen wat bollebozen bij elkaar.

Vaak wordt als voorbeeld van de 'wisdom of crowds' het raden van het gewicht van een koe of het aantal knikkers in een pot gegeven. Het gemiddelde van de individuele schattingen zou dan een nauwkeurig antwoord op moeten leveren. Onafhankelijkheid en diversiteit is daarbij essentieel. Maar de 'wisdom of crowds' is meer dan dat. In dit artikel laat ik zien wat de 'wisdom of crowds' kan betekenen voor veiligheid en hoe de nabije toekomst er op dit terrein uit zou kunnen zien. En die toekomst is dichterbij dan u denkt.

## Burgers voor het karretje spannen

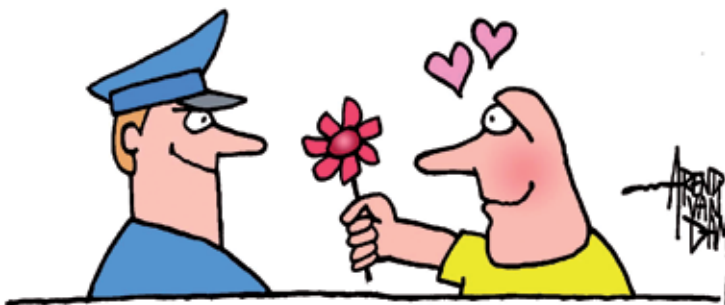
De manieren om de 'wisdom of crowds' te benutten bestrijken een spectrum van crowdsourcing via cocreatie tot en met zelforganisatie, met steeds een toenemende invloed van de 'crowd' op het proces. Het meest gebruikt is crowdsourcing: het betrekken van (uitbesteden van een taak aan) een grote groep als hulpbron van ideeën, kennis, productie, uitwisseling en verspreiding. Losse, individuele bijdragen worden daarbij geëxperimenteerd tot iets gezamenlijks. Op heel veel terreinen is geëxperimenteerd met crowdsourcing, ook op het vlak van wetgeving en opsporing. Zo is er de website [internetconsultatie.nl](http://internetconsultatie.nl) waar burgers

kunnen bijdragen aan het verbeteren van wet- en regelgeving die in voorbereiding is. Het idee is dat burgers verfrissende ideeën en oplossingen kunnen hebben die een waardevolle aanvulling kunnen zijn op die van de juridische beleidsmakers en experts. Een ander bekend en succesvol voorbeeld is de meldings-app van de politie waarmee burgers melding kunnen maken van vernielingen, ongelukken of incidenten in de stad. Extra ogen en oren dus.

Nog een heel ander voorbeeld is de manier waarop eBay haar eigen gebruikers inzet bij het oplossen van geschillen tussen kopers en verkopers. Jaarlijks zijn dat er zo'n zestig miljoen, teveel om allemaal zelf af te handelen. Daarom maakt eBay gebruik van zogenaamde 'crowdsourced online dispute resolution': een willekeurige gebruiker, die niets te maken heeft met het betreffende geschil, wordt gevraagd om de situatie te beoordelen. Uiteindelijk doen zo 12 tot 13 gebruikers een uitspraak die leidt tot een bindende uitspraak voor het geschil: een vorm van rechtspraak met een publieksjury.

Deze voorbeelden laten de variatie aan mogelijkheden zien die internet en sociale media met zich meebrengen. Aan de ene kant kunnen burgers meer betrokken worden, aan de andere kant kunnen burgers ook meer van zich laten horen, zich organiseren en laten ze zich daarbij niet volledig sturen of in een hokje plaatsen. Dat betekent dat organisaties, of het nu bedrijven zijn of overheden, grip op burgers verliezen, als ze die al hadden. Project X in Haren laat zien hoe een online vergissing kan uitlopen op echte incidenten: het gevolg van een niet op voorhand te voorspellen wisselwerking tussen online en offline gedrag. Wat betekent dit voor de toekomst?

<sup>1</sup> De auteur deed de afgelopen jaren onderzoek naar het fenomeen 'wisdom of crowds'. Van zijn hand verschenen de boeken *Samen slimmer: hoe de wisdom of crowds onze samenleving zal veranderen* en *Veel gekwetter, weinig wol: de inzet van sociale media door overheid, politiek en burgers*. Meer informatie via <http://wisdomofthecrowd.nl>.



### Nieuwe technologische ontwikkelingen

In de toekomst wordt het menselijk gedrag steeds beter te meten en te sturen. Dat komt door uiteenlopende technologische ontwikkelingen. Zo wordt het door de opkomst van zogenaamde 'big data' mogelijk om grote hoeveelheden data te verwerken en daaruit informatie en kennis te halen. Deze ontwikkeling is bijzonder krachtig in combinatie met twee andere: de opkomst van steeds meer sensoren in de openbare ruimte: camera's, microfoons en ecosensors, zowel in gevels, gebouwen als op de smartphones. Dit betekent dat er steeds meer data gegenereerd worden, en daarmee dus informatie beschikbaar komt over wat er in de omgeving gebeurt.

Tegelijkertijd wordt de software om deze data te analyseren krachtiger en 'socialer': deze is steeds beter in staat om ook taal te begrijpen. Deze software wordt nu al gebruikt om sociale media berichten zoals tweets, blogs en statusupdates bij Facebook, te analyseren. Daarmee kan van iedere burger een profiel gemaakt worden en uit grote hoeveelheden berichten kunnen populaire thema's worden gehaald of beginnende onrust gesignaleerd worden. Tel hierbij op de groeiende rekenkracht op waarmee het mogelijk wordt om de

structuur van sociale netwerken en interacties in kaart te brengen en de dynamiek ervan live te volgen of prognoses te maken hoe ze zich gaan ontwikkelen.

Niet alleen bedrijven met hun marketingwensen, maar ook overheden kijken verlekkerd naar deze nieuwe technologische mogelijkheden en ontwikkelen nieuwe toepassingen om sociale media nog uitgebreider te monitoren. Het is de bedoeling om hiermee vroegtijdig onrust of incidenten op te sporen en de ontwikkeling ervan (escalatie, groeit het of verdwijnt het?) te volgen. In een nog verdere toekomst zullen nieuwe technieken zoals hersenscans nog eerder kunnen zien aankomen als mensen van sentiment veranderen. En de technieken om het gedrag van mensen te sturen door middel van beeld, geluid en anders, groeien. Zo is bekend dat mensen vredelievender worden als ze gespoten worden met het middel oxytocine, een neurotransmitter, die de emotionele binding tussen mensen vergroot.

### Minority Report als toekomstscenario?

En voilà, het scenario uit de film *Minority Report* is geboren: de belofte van een misdaadvrije wereld door 'precrime': het opsporen en ingrijpen voordat een misdaad is begaan. Toch blijkt dat geen systeem feilloos is en dat mensen de zwakste schakel blijven. Niet alleen brengt het gebruik van deze technieken grote vragen met zich mee op het vlak van privacy, maar ook de vraag hoe voorspelbaar 'misdad' is. Ons gedrag is niet eenduidig vast te stellen op basis van onze tweets of de uitslag van onze lichaamssensoren en hersenscans. Je kunt niet van tevoren voorspellen of wat begint als een feestje uitloopt op rellen of vandalisme. Niet ieder Project X-feestje loopt uit op ellende.

Belangrijk is daarom het besef dat het inzetten op het monitoren van burgers alleen geen heil brengt. Kijkend aan de zijlijn en wachtend wat er gaat gebeuren. Het lijkt toekomstmuziek maar blijkt dit vooral de richting te zijn waar veel overheden naar kijken in hun veiligheidsprojecten. Hoog tijd dus dat er ook aan alternatieve strategieën voor de toekomst wordt gewerkt om de veiligheid te vergroten. Daarbij kunnen we leren van initiatieven als Burgerwacht: door burgers niet af te tappen, maar te investeren in de zelfredzaamheid en het zelforganiserend vermogen van burgers. Daarvoor moeten we kijken naar een andere kant van de wisdom of crowds: de interacties tussen mensen. Hoe kunnen deze interacties 'slimmer'? Diezelfde technologische ontwikkelingen zouden ook ingezet kunnen worden om de interactie tussen mensen te bevorderen: wederzijds begrip, leren luisteren, feedback, de-escalatie en verbroedering.

Investeren in het versterken van mensen in plaats van het versterken van systemen die buiten mensen staan. Uiteindelijk zit de wijsheid in ons allemaal. Dát is wat mij betreft de echte 'wisdom of crowds'.



# The Hague Security Delta

## ontwikkelt campus voor innovatie en veiligheid

**Henk Kool,**  
wethouder Sociale Zaken,  
Werkgelegenheid en  
Economie van Den Haag

Gerichte investeringen in innovatieve veiligheidsoplossingen zijn hun bestedingen dubbel en dwars waard. Er is immers geen sector waar het rendement in zowel maatschappelijk als in economisch opzicht zo goed hand in hand gaan als in de sector veiligheid. Op papier is de buit dus al binnen. Maar in de praktijk is er werk aan de winkel.

Het maatschappelijke rendement van investeringen in oplossingen rond veiligheid bestaat uiteraard uit een veiliger maatschappij, een veiliger Nederland. Het is dus topprioriteit voor de nieuwe landelijke veiligheids-campus om zo goed mogelijk in te spelen op de behoeftes van overheden, diensten en organisaties die actief zijn in het veiligheidsdomein. Het economische rendement bestaat uit de versterking van de internationale concurrentiepositie van de BV Nederland. Het sleutelwoord dat deze doelen verbindt is publiekprivate samenwerking.

The Hague Security Delta, het nationaal veiligheidscluster in de Haagse regio, ontwikkelt een campus voor innovatie en veiligheid, die faciliteiten en netwerken op één locatie biedt. En daar is een moderne publiekprivate samenwerking mogelijk. De Gouden Driehoek (overheid, onderzoek/onderwijs en bedrijven) in veiligheid

bestaat immers wel, maar functioneert niet optimaal. En dat is een belangrijke voorwaarde voor de verdere ontwikkeling van deze sector. Veiligheidsvraagstukken zijn tegenwoordig complex van aard, zij vragen om oplossingen met een hoog high tech karakter. De kennis van instituten en het bedrijfsleven zijn daarom dus onmisbaar!

De campus voor innovatie en veiligheid wordt een omgeving waar uiteenlopende initiatieven in het veiligheidsdomein elkaar letterlijk ontmoeten. De kern wordt gevormd door living labs, innovatie staat er centraal. Zo zijn er plannen voor een seriousgaming lab, een real time intelligence lab en een cyber security experience lab. Naast de campus voor innovatie en veiligheid werken wij met onze partners ook aan andere initiatieven die het veiligheidscluster zullen versterken. Daarnaast werken we met partners aan de oprichting van een

Cyber Security Academy op deze campus. In datzelfde gebouw wordt ook het nieuwe kantoor van The Hague Security Delta (HSD-Office) gehuisvest, evenals een MKB-desk en het European Network for Cyber Security (ENCS).

Ik ben heel trots dat we met The Hague Security Delta dit soort unieke initiatieven van de grond krijgen. Zij sluiten naadloos aan op ons profiel van Den Haag, internationale stad van vrede en recht. Dit veiligheidscluster is er om de landelijke samenwerking in het veiligheidsdomein te versterken. Dit is van groot belang voor de economie en voor onze internationale concurrentiepositie.

Dit jaar wordt het begin van de campus voor innovatie en veiligheid zichtbaar! Het is een prachtige plek om te etaleren, te innoveren en te realiseren. U bent van harte welkom!

## Hou veiligheid in de gaten inkoopinnovatie urgent

Afgelopen december was daar eindelijk het moment waar we lang naar hadden uitgezien: Enschede was de trotse gaststad van het Glazen Huis 2012. Er is in zes dagen tijd een recordbedrag van €12 miljoen bij elkaar gebracht voor het Rode Kruis. Onze gezellige en gastvrije stad is bezocht door ruim een half miljoen bezoekers. Voor de veiligheid van bezoekers van evenementen draagt de lokale overheid samen met de organisatoren een verantwoordelijkheid. Dat is een serieuze aangelegenheid blijkens de druk op de openbare veiligheid van de afgelopen jaren. Een uit de hand gelopen strandfeest, noodweer tijdens festivals en het nieuwe fenomeen van de X party in Haren als een negatieve uitwas van de moderne communicatietechnologie.

Maar gelukkig kun je innovatieve technologie ook op een positieve wijze inzetten om onveiligheid te signaleren en zo mogelijk te voorkomen. In Enschede is dat gedaan. In samenwerking met de Veiligheidsregio is in het stadhuis een crowd controlroom ingericht met een aantal innovatieve systemen. Samenwerking van partijen maakte mogelijk om continue een zo accuraat mogelijk beeld te verkrijgen van de actuele situatie tijdens het evenement Serious Request van Radio 3FM. En dat was nodig met een half miljoen bezoekers die verspreid over al die dagen zijn geweest.

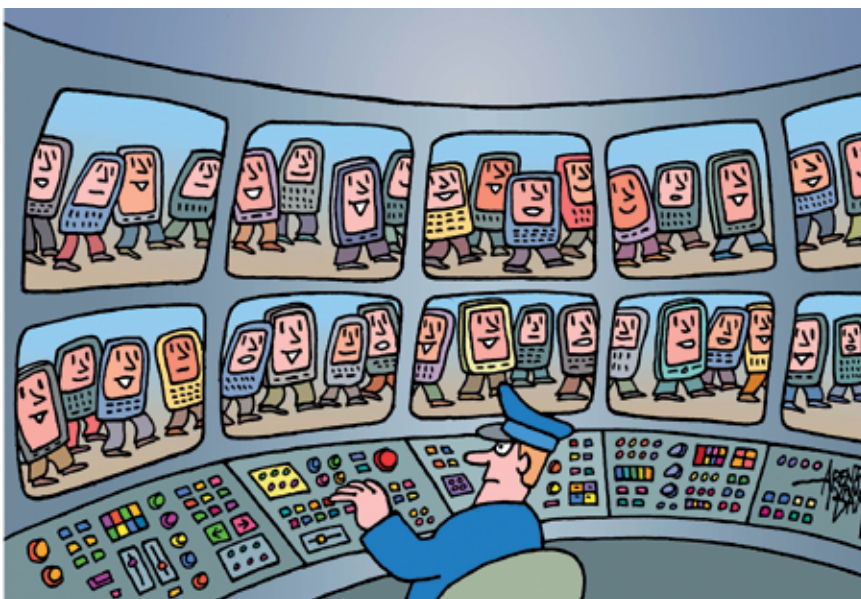
In Enschede is gebruik gemaakt van het innovatieve systeem om bezoekersaantallen te tellen en bewegingen van massa's te monitoren. Dat kan met sensoren die het signaal afkomstig van smartphones registreren. Dit gaf informatie over waar de menigte zich in de binnenstad concentreerde en welke routes intensiever werden gebruikt. Hiermee konden hulpverleners tijdig vaststellen of een bepaald plein qua bezetting aan de veiligheidslimiet zat of dat er elders een grote oploop kon worden verwacht. Tijdige verzending van waarschuwingen via Twitter aan het publiek en gerichte

berichten op de tekstkarren waren mogelijk om de mensenmassa's te bereiken en advies te geven over de drukte.

Ook is gebruik gemaakt van het slimme Twitcident. Twitcident analyseert en filtert Twitterberichten op relevante informatie over de actuele situatie, hoe de burgers dit ervaren en welke informatiebehoefte zij hebben, hiermee ontstaat een overzicht van potentiële dreigende omstandigheden. Met de inzet van het Urban Shield systeem was voortdurend de exacte positie van hulpverleners in 3D te zien op een scherm in de crowd controlroom. Deze stond in direct contact met de eenheden van de stadswacht, politie en brandweer zodat die bij incidenten zeer snel ter plekke konden zijn. Het uitlezen van de in het centrum aanwezige beveiligingscamera's in dezelfde crowd controlroom maakte het zicht op de veiligheid in de stad compleet.

Met de beschikbare informatie via sensoren, Twitcident en het Urban Shield systeem waren de verschillende professionals en hulpverleners in staat om effectiever onveilige situaties te voorkomen en sneller in te grijpen bij incidenten dan zonder deze informatie. Dit droeg niet alleen bij aan het vergroten van de veiligheid van de bezoekers maar ook die van de hulpverleners. Heel logisch toch om dan bij evenementen als deze gebruik te maken van de beschikbare technologie?

Toch is dat niet vanzelfsprekend. De vraag is: wie betaalt de rekening? Reden voor het seminar Innovatieve Oplossingen in het Veiligheidsdomein tijdens Serious Request. Er is grote behoefte om de inkoopkracht te bundelen en te delen. Zonder die bundeling komt de markt onvoldoende op gang. Bovendien is het te overwegen om het gebruik van crowd control technologie bij grote evenementen te gaan verplichten. Dat zijn conclusies van het gesprek tussen specialisten van overheid en bedrijfsleven tijdens het seminar. Een nauwe samenwerking met gemeenten en het Ministerie van Veiligheid en Justitie en het bedrijfsleven is nodig om tot een verbetering van de inkoop van innovatieve veiligheidsdiensten te komen; inkoopinnovatie urgent!



crowd control

# Defensie en innovatie

Bij een modern en welvarend land als Nederland hoort ook een moderne krijgsmacht. Een krijgsmacht die Nederlanders bescherming biedt en, in internationale samenwerkingsverbanden als NAVO en EU, onze vitale belangen veiligstelt. Wat Defensie doet moet zij goed doen. Het worden van “goede tweede” is in het krijgsbedrijf nu eenmaal geen optie. Een krijgsmacht die ertoe doet moet er daarom altijd naar streven de beste te zijn. Dit betekent dat bij het uitvoeren van operaties alleen het beste goed genoeg is.

*ir P.J. (Jelle) Keuning,  
souschef Ressort DR&D,  
Ministerie van Defensie*

Om hier invulling aan te kunnen geven moet Defensie voorbereid zijn op voorziene en onvoorziene omstandigheden en veranderingen in de wereld. Waar het om gaat is aanpassingsvermogen, “survival of the fittest” betekent dat degene die het best weet in te spelen op veranderende omstandigheden zal overleven.

Maar er is nóg een reden voor innovatie. Gezien de krimpende budgetten is Defensie genoodzaakt haar efficiency steeds kritischer te bezien. Innovatie kan ook een belangrijke bijdrage leveren aan kostenbeheersing. Dat verklaart waarom er binnen Defensie altijd een grote aandacht is geweest voor het innovatieve vermogen. Defensie ziet het belang van kennis en innovatie, gericht op de slimme inzet van geavanceerde technologie. En ondanks alle veranderingen die op Defensie afkomen, blijft dit ook in de komende jaren onverminderd van kracht. Hiertoe is wel een visie, richting en duidelijkheid vereist. Met de Strategie-, Kennis- en Innovatieagenda van Defensie (de SKIA) wordt hieraan een bijdrage geleverd.

## SKIA

De SKIA is een afgeleide van de beleidsbrief van het vorige kabinet over de toekomst van de krijgsmacht. Tegelijk met de beleidsbrief heeft Defensie in 2011 ook deze SKIA uitgebracht. In de SKIA wordt strategievorming, kennis en innovatie in een samenhangende benadering bijeen gebracht. Dit vanuit het besef dat er een nauwe samenhang bestaat tussen deze drie. Kennis is zowel nodig om de strategie te kunnen bepalen als om deze te kunnen uitvoeren. Innovatie ligt met name in de sfeer van toepassing, maar kan alleen tot stand komen indien de benodigde kennis en technologie beschikbaar zijn. Kennis en innovatie staan ten dienste van zowel het ontwikkelen als het uitvoeren van de door de politiek vastgestelde strategie.

De SKIA dient de volgende doelen.

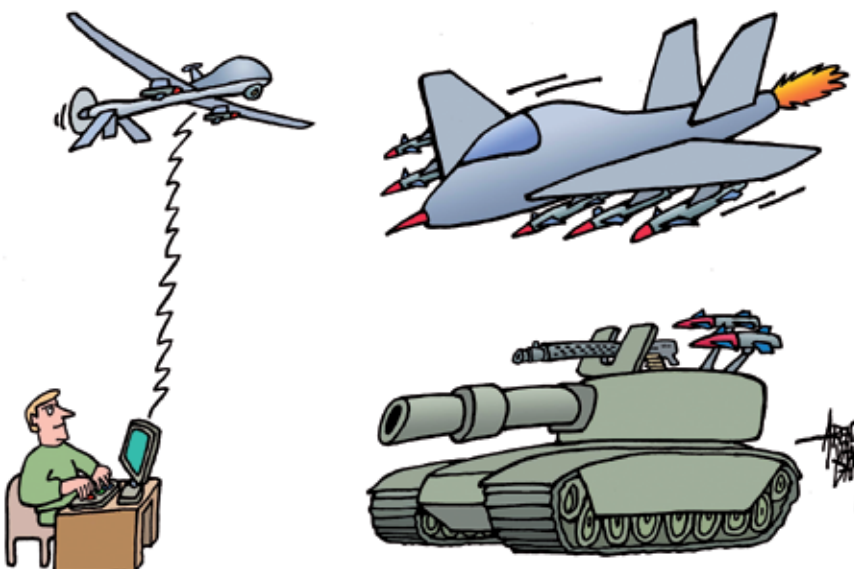
1. het versterken van de strategische functie, om zeker te stellen dat de juiste keuzes gemaakt worden in een steeds veranderende wereldbeeld;
2. het richten van de kennisontwikkeling. Nauwe samenwerking van Defensie met de kennisinstututen (TNO, NLR, MARIN) krijgt vorm in een strategisch partnerschap. De SKIA stuurt de kennisopbouw door een viertal kennisprioriteiten te identificeren. Deze kennisprioriteiten zijn een afgeleide van de door de politiek vastgestelde strategische doelstellingen;
3. het stimuleren van innovatie. Om het innovatieve karakter van Defensie te ondersteunen en te versterken geeft de SKIA specifieke innovatiedoelen. Deze innovatiedoelen liggen in het verlengde van de strategische doelstellingen, zoals deze verwoord zijn in de beleidsbrief.

Met de SKIA geeft Defensie daarmee voor de komende jaren richting aan kennis en innovatie.

## Innovatie

Innovatie betreft het introduceren van nieuwe ideeën, technologieën, materieel, diensten en processen. Het is de laatste stap in een proces dat begint bij kennis, een vervolg krijgt in technologieontwikkeling en via prototypeontwikkeling uiteindelijk resulteert in de gewenste innovatie als het product geïntroduceerd wordt op de markt. De SKIA identificeert vier innovatiedoelen waarop Defensie zich de komende jaren zal richten:

- informatiegestuurd optreden in netwerken;
- effectieve beïnvloeding van operaties;
- energiebewuste krijgsmacht;
- een innovatieve en flexibele organisatie.







Patrouilleschip Holland

Innovatie vindt plaats in de Gouden Driehoek. Defensie doet dit te zamen met het bedrijfsleven en de kennisinstututen. Defensie heeft daarom belang bij een goed functionerende gouden driehoek en is ook bereid daarin te investeren. Dit krijgt vorm in de Defensie Industrie Strategie (DIS). Gezien de krimpende budgetten is Defensie wel genoodzaakt haar eigen rol binnen deze Gouden Driehoek. Defensie doet dit te zamen met het bedrijfsleven en de meer dan in het verleden te verleggen van *smart designer/specifier* naar *smart user/buyer*. Dit verandert ook de rol van de andere partijen, steeds meer zullen zij worden uitgenodigd aan de voorkant te gaan meedenken in het behoeftstelling-proces. Het meedenken wordt mede vorm gegeven in processen zoals Concept Development and Experimentation (CD&E), dat binnen Defensie steeds vaker wordt toegepast. Dat dit beleid zijn vruchten afwerpt wordt geïllustreerd aan de hand van twee recente materieel-projecten.

#### VOSS

Het project Verbeterd Operationeel Soldaat Systeem (VOSS) richt zich op het verbeteren van de persoonlijke uitrusting van de soldaat, met name op het gebied van mobiliteit, bescherming en informatievoorziening. De sleutel tot effectief optreden ligt bij snelle informatie, de innovatie richt zich op het verbeteren van de situational awareness (SA). Hoe te komen tot een geïntegreerd beeld in de commandolijn vanuit vele sensoren en informatiebronnen. Daarnaast blijft mobiliteit essentieel voor soldaatoptreden. Indien er te veel gedragen moet worden lijdt de gevechtsprestatie daaronder. Innovaties in bescherming bieden de mogelijkheid de belangrijkste onderdelen van het lichaam redelijk te beschermen, zonder dat dit de mobiliteit te veel verslechtert. Dit alles heeft geresulteerd in een nieuwe uitrusting, lichter en slimmer, waarbij de SA toeneemt. Zo wordt zowel de slagkracht als de veiligheid vergroot.

#### Patrouilleschip Holland

Het nieuwe Patrouille Schip (PS) van de Koninklijke Marine is een uniek innovatief concept, mogelijk

gemaakt dankzij de beproefde gouden driehoek binnen het Nederlands Maritieme Cluster voor de zelschepende marinebouw in Nederland. Het innovatieve karakter van het schip komt bijvoorbeeld tot uitdrukking in het bemanningsconcept. Dankzij de revolutionaire inrichting kan de scheepsbemanning teruggebracht worden tot slechts 50 man, ongeveer een derde van de huidige bemanningen. Het schip is ook uitgerust met een geïntegreerde mast voor alle sensor-, communicatie- en radarsystemen. Dankzij deze mast kan het PS tot dicht onder de kust worden ingezet, zorgen voor een perfect zeebeeld en kunnen kleine objecten en dreigingen op korte afstand automatisch ontdekt worden. Het innovatieve karakter wordt onderstreept doordat het PS in 2012 is bekroond tot "Schip van het jaar".

#### Samenwerking

Er is een groeiende technologische overlap tussen de terreinen defensie en veiligheid, de welbekende dual-use technologieën. Was in het verleden op veel voor de krijgsmacht relevante technologiegebieden de ontwikkeling afhankelijk van de Defensie-inspanning, tegenwoordig is in toenemende mate de civiele ontwikkeling zowel in omvang als qua snelheid leidend. Defensie streeft daarom naar maximale aansluiting bij de civiele ontwikkelingen. Dit wordt op meerdere plaatsen zichtbaar, internationaal binnen de Europese kaderprogramma's en nationaal binnen het Topsectorenbeleid. Door samen te werken bij de ontwikkeling en innovatie, die voor Defensie en andere departementen belangrijk zijn, kunnen de schaarse financiële middelen effectiever ingezet worden. In de SKIA wordt in dat kader onderzoek op het gebied van bescherming tegen chemische en biologische dreigingen, het gebruik van de ruimte en cyber security genoemd. Er wordt daarom geïnvesteerd in een groeiende samenwerking met de betrokken ministeries, onder meer tot uitdrukking komend in het project Versterking Civiel-Militaire Samenwerking (VCMS). R&D-samenwerking is daarbinnen één van de onderwerpen die door Defensie nadrukkelijk wordt gezocht.

**Peter de Beijer,**

projectleider Internet Research Network iRN Politie en

projectleider Verduurzaming iRN/iColumbo TNO

# Internet gedreven innoveren vergroot veiligheid

De overheid kan veel, heel veel leren van het Internet. Het heeft namelijk een aantal zeer aantrekkelijke karakter eigenschappen (open, anarchistisch, snel, grenzeloos, plat georganiseerd) die overheden traditioneel onvoldoende hebben maar die wel enorm kunnen helpen succesvol te innoveren. Successen op het Internet ontstaan meestal door een combinatie van die unieke karaktereigenschappen van het Internet, gecombineerd met visie, enthousiasme en vasthoudendheid bij de mensen die ontwikkelen, uitvoeren en sturen.

### **iRN: Internet Research Network**

Het iRN is een, bij de politie ontwikkelde, netwerk infrastructuur voor onderzoek op Internet. Het wordt gebruikt door een breed scala aan overheidsdiensten uit de veiligheidsector, die zich bezig houden met toezicht, handhaving en opsporing. Het iRN is ook een, op Internet geïnspireerd, platform met een community van inmiddels meer dan 6000 gebruikers die vertrouwd kennis delen en online samen werken. Het iRN is daarnaast ook nog een omgeving waar veel innovatieve nieuwe technologie, diensten (op basis van open source software) en methoden worden ontwikkeld door een community van ontwikkelaars (wetenschappers, software developers, bedrijfsleven). Binnen het iRN zijn de karaktereigenschappen van het Internet en de successen van Internet bedrijven, -organisaties en -projecten dagelijks leidend in wat we doen en dé inspiratie voor hoe we georganiseerd willen zijn, hoe we naar ontwikkeling kijken, hoe we innoveren en waarom we een community moeten zijn met onze gebruikers en partners. Die combinatie leidt namelijk tot voortdurend snelle, vernieuwende innovatieve diensten en meer kennis voor alle iRN gebruikers,

waarmee hun dagelijkse werk binnen het veiligheidsdomein bij de overheid voortdurend beter uitgevoerd kan worden.

Een mooi voorbeeld is de toepassing van open source big data technologie (dezelfde technologie waarop Google, Twitter en Facebook gebaseerd zijn) voor onderzoek van grote hoeveelheden informatie. Vanuit iRN ontwikkelen wij op basis van deze technologie volgens de scrum methode<sup>1</sup> toepassingen voor Internet onderzoek (onder de verzamelnaam iColumbo). De iColumbo technologie is, naast haar toepassing in het iRN, ook prima geschikt voor verwerking en analyse van andere data verzamelingen bij de overheid. Wij delen deze technologie dan ook kosteloos met andere overheidsdiensten en we geven aanpassingen of uitbreidingen op open source software terug aan de Internet community. De afspraak is dat elke verdere ontwikkeling van de iColumbo technologie weer kosteloos met ons wordt gedeeld. Daarmee creëren we een duurzaam innovatief gedistribueerd 'ontwikkel' ecosysteem van technologie en kennis, waarbij we tegen vrij lage kosten (licentiekosten vrij) de community van iRN gebrui-

kers bij alle aangesloten overheidsdiensten voortdurend van nieuwe en verbeterde toepassingen en kennis kunnen voorzien.

### **Organiseer volgens het Internet**

Om succesvol te innoveren volgens 'het Internet model' is het belangrijk dat de organisatiestructuur daar op ingesteld is of in ieder geval daarvoor de ruimte en het vertrouwen kan geven. Dat is bij veel overheidsdiensten een grote uitdaging omdat de organisatiestructuren en gedachten over sturing en controle nogal haaks staan op dit platte, snelle netwerkorganisatiemodel. Toch is het, om bij te blijven met alle snelle ontwikkelingen, zeker die van het Internet, geen echte keuze. Het Internet dwingt, ook overheidsorganisaties, om na te denken over hoe wij georganiseerd zijn, hoe we succesvol innovatief en kosten efficiënt kunnen zijn en of we ons niet veel intensiever als een community moeten gaan gedragen, waarbij we onze kennis en ontwikkelingen voortdurend delen. Succesvol, sneller, goedkoper en beter innoveren met als inspiratie het Internet model biedt de mogelijkheid, ook voor de veiligheidsector bij de overheid. Het vraagt mogelijk wel om andersoortige kennis en de nodige aanpassingen in de manier waarop we georganiseerd zijn om het daadwerkelijk te gaan doen.

Beth Noveck, voormalig plaatsvervangend Chief Technology Officer in de Obama regering hield in juni 2012 een TED Talk over het Open Government Initiative. Zeker de moeite waard om even online<sup>2</sup> te bekijken en geïnspireerd te raken.

<sup>1</sup> [http://nl.wikipedia.org/wiki/Scrum\\_\(softwareontwikkelmethode\)](http://nl.wikipedia.org/wiki/Scrum_(softwareontwikkelmethode))

<sup>2</sup> [http://www.ted.com/talks/beth\\_noveck\\_demand\\_a\\_more\\_open\\_source\\_government.html](http://www.ted.com/talks/beth_noveck_demand_a_more_open_source_government.html)

dr. ir. Mark van Staalduinen,  
innovatieconsultant TNO  
(Mark.vanStaalduinen@tno.nl)

# Succesvolle innovatie vereist diversiteit en continuïteit!

Het Internet verandert de wereld razend snel. Wie kon een paar jaar geleden bedenken dat bijna iedereen in het bezit is van een smartphone en continu actief is in sociale netwerken? Dat alle TV's connected zijn en dat wij voornamelijk online winkelen en betalen? Als gevolg daarvan ontstaan grote hoeveelheden data in open bronnen, met consequenties voor de veiligheid van burgers en de maatschappij. Vanuit TNO werken we aan intelligente tooling, die ondersteuning biedt bij het duiden en interpreteren van die data binnen de juridische, privacy en forensische kaders. Dit noemen we *media mining*. De afgelopen twee jaar hebben we in opdracht van de NCTV in samenwerking met verschillende veiligheidsdiensten gewerkt aan een aantal innovatieve tools.

Niet elke website is eenvoudig te analyseren, zoals Flash websites. De meeste zijn zelfs niet doorzoekbaar met Google. Deze webtechnologieën worden bewust ingezet om informatie te presenteren voor mensen, die onzichtbaar is voor computers. De conclusie leidde tot een slimme "clickbot", die als een mens door een website klikt en alle binnenkomende data afvangt. De ontwikkelde testsoftware verzamelt significant meer data dan standaard oplossingen. Diversiteit van mogelijke oplossingen is bereikt door een inspiratielunch, waar verschillende diensten hun ervaringen konden delen. Daarnaast is een workshop georganiseerd door het Public Services Innovation Center (PSIC), waar studenten samen met domeinexperts hebben meegewerkt. Omdat de oplossing menselijk gedrag vertoont, blijkt het ontwikkelde mechanisme ook geschikt voor andere toepassingen, bijvoorbeeld om honeypots<sup>1</sup> te versterken.

Naast tekst staat het internet vol met foto's en video's. Er zijn weinig tools, die de potentie van dit beeldmateriaal benutten. Binnen het beeldmerkenproject zijn drie ICT-diensten onderzocht aan de hand van het STOF-model. Dat model stelt dat een ICT-dienst succesvol kan worden als de

geboden dienst (Service) waardevol is, de Technologie werkt, de Organisatie van gebruikers en leveranciers op orde is en de Financiën passend zijn. Dit verklaart, waarom verschillende projecten niet tot bruikbare tools hebben geleid, omdat veelal op één domein wordt gefocust. Drie diensten zijn uitgewerkt: locatieherkenning met Twitter-foto's, scannen van nieuwe YouTube video's en het spotten van trends in beeldmateriaal. Conclusie: de operationele kosten zijn van die orde dat zij op nationale schaal te realiseren moeten zijn.

Sinds 2011 werkt TNO als strategisch kennispartner mee aan het iRN (Internet Research Network, zie het artikel van Peter de Beijer). Het iRN levert diensten aan ongeveer 6000 gebruikers bij verschillende overheden die toezicht-, opsporing- en handhavingstaken hebben op het internet. Van politie, Belastingdienst en DNB tot en met gemeenten. Binnen het iRN wordt een innovatieve dienst ontwikkeld voor de ondersteuning van internetonderzoek: iColumbo. Kortom, innovatie is essentieel voor het iRN, en daarom is de samenwerking met TNO vruchtbaar. Het iRN biedt een landingsplaats en inspiratiebron voor innovatieve oplossingen, waarmee continuïteit ontstaat in de innovatieketen van wetenschappelijk

onderzoek tot de nieuwste oplossingen voor eindgebruikers.

Wat maakt innovatie succesvol? Essentieel zijn: diversiteit en continuïteit. Diversiteit in mensen, expertises, organisaties, functies en processen. Diversiteit binnen het projectteam, maar ook in de contacten tussen het team en de dagelijkse praktijk om zoveel mogelijk goede ideeën door te laten dringen en tunnelvisie te voorkomen. Diversiteit is essentieel om de juiste oplossing te vinden. Continuïteit is vereist in het projectteam, de doelstelling en vooral in de innovatieketen richting eindgebruikers. Dit betekent dat innovatieve oplossingen een landingsplaats vereisen. Niets is frustrerender dan resultaten boeken, die niet gebruikt worden. Continuïteit is essentieel, zodat een goede oplossing ook waardevol kan worden.



<sup>1</sup> Een opzettelijk zwak beveiligd systeem dat opgezet wordt om computercriminelen, virussen, Trojans en dergelijke te kunnen detecteren.

# Open innovatie in een gesloten omgeving

Innovatie is van levensbelang voor organisaties. We kennen de bekende voorbeelden van de Senseo van Philips en Sara Lee en de Ipad van Apple. Ook de overheid laat zich niet onbetuigd; denk aan de belastingdiskette en de Zandmotor voor de kust van Zuid-Holland.

In het bedrijfsleven heeft innovatie zich ontwikkeld van een hoofdzakelijk interne aangelegenheid naar een activiteit die deels is geoutsourced waardoor er uitgebreide samenwerkingsverbanden zijn ontstaan voor het ontwikkelen van nieuwe producten en diensten. De vraag rijst of en hoe de overheid in het algemeen en de gesloten inlichtingendiensten in het bijzonder in deze 'open innovatie'-trend moeten meegaan.

**Patrick van der Duin,**  
TU Delft  
**Frank Bacco,**  
Bestuursstaf, Ministerie  
van Defensie

Open innovatie houdt in dat organisaties innovatieprocessen delen met andere organisaties. Niet uit vrijgevigheid maar, onder andere, omdat moderne technologie ervoor heeft gezorgd dat het vrijwel onmogelijk is om informatie en kennis binnenkamers te houden en omdat kenniswerkers niet meer hun volledige arbeidzame leven bij één werkgever doorbrengen. Voor organisaties is het daarom verstandiger en efficiënter om aan te haken bij deze ontwikkeling en het ideaal van geheime en vertrouwelijke innovatieprocessen, waarmee een voorsprong op de concurrent zou kunnen worden opgebouwd en vastgehouden, op te geven. Door kennis ten behoeve van innovatie te delen met andere organisaties kan een organisatie haar eigen kennispotentieel vergroten.

Enkele kanttekeningen vooraf. Allereerst is open innovatie niet in alle gevallen een handige strategie. Henry Chesbrough, de grondlegger van het concept, schrijft in het begin van zijn boek *Open Innovation* dat in sectoren met onder andere, een beperkte arbeidsmobiliteit, een beperkt aantal 'start-ups' en waarin universiteiten geen belangrijke rol spelen, gesloten innovatie beter is. Voorbeelden zijn kerncentrales en de mainframe computerindustrie. Open innovatie is dus niet het antwoord op alle innovatieproblemen.

Verder wordt bij open innovatie nog steeds uitgegaan van de opvatting dat innovatieprocessen lineair zijn. Maar dit is een al te simpele opvatting van een activiteit die gekenmerkt wordt door *trial and error* en waar, in tegenstelling tot projecten, niet van te voren vaststaat wat de uitkomst is. Tot slot wordt open innovatie vaker

met de mond beleden dan in de praktijk uitgevoerd. Een goed voorbeeld hiervan zijn de patentoorlogen tussen Samsung en Apple, terwijl juist het laatste bedrijf vaak genoemd wordt als exponent van de open innovatiegedachte. Ruzie maken over patenten is immers iets wat niet goed past bij het vrij delen van kennis en informatie wat de essentie is van open innovatie.

## Wat kan open innovatie betekenen voor de overheid?

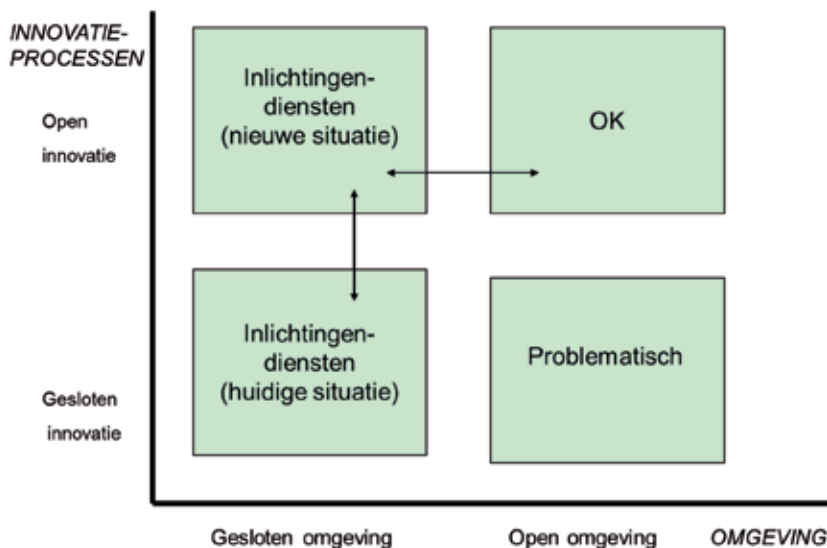
Open innovatie betekent in feite het einde van de dominantie op innovatiegebied van grote bedrijven die beschikken over ruime R&D-budgetten. Kennis- en informatiedeling vindt zijn pendant in de (politieke) machtsverschuivingen naar lokale overheden en de privatisering en verzelfstandiging van overheidsdiensten. En net zoals grote bedrijven niet meer de dienst uitmaken in veel markten is ook de maakbaarheid van de samenleving door de overheid sterk verminderd. De samenleving is open geworden. Dit heeft als direct gevolg dat besluitvormingsprocessen door de overheid niet automatisch topdown verlopen en dus niet lineair. Ook bij de overheid is besluitvorming een complexe aangelegenheid geworden die niet eenvoudig volgtijdelijk kan worden beschreven. De kennisvoorsprong van de overheid ten opzichte van de burger is grotendeels verdampt doordat burgers mondiger zijn geworden en door wettelijke arrangementen als de Wet Openbaarheid van Bestuur (WOB). Voor de inlichtingendiensten geldt specifiek dat er sinds '9/11' een verschuiving heeft plaatsgevonden van een 'need to know' naar een 'duty/dare to share' cultuur waardoor kennis minder exclusief in kleine compartimenten wordt vastgehouden en meer voor een groter domein toegankelijk is. Het ontstaan van de Nationaal Coördinator Terrorismebestrijding is daarvan een goed voorbeeld. Kennisvermeerdering ontstaat minder door het apart verzamelen en verrijken van informatie en het exclusief voor je zelf houden maar meer door het handelen in kennis en gebruik maken van elkaars puzzelstukjes.

Open innovatie is dus een potentieel interessante innovatiestrategie voor de overheid en dus in principe ook voor de inlichtingendiensten. Hoe kan men dat gebruiken gezien het specifieke vertrouwelijke karakter van haar activiteiten? Allereerst zijn er al diverse innovatieprocessen die opener zouden kunnen zoals alle overheidsinspanningen op offensieve en defensieve

cyberactiviteiten. Het speelveld in dit domein is beter te vergelijken met een pokerspel dan met een schaakspel. Bij een pokerspel is het niet duidelijk welke troeven de tegenstander in zijn hand heeft. Bij een schaakspel kun je in principe alle zetten voorspellen en je weet welke zetten de tegenstander kan doen. In de nog onbekende dynamiek van cyberactiviteiten is open innovatie beter op zijn plaats dan gesloten innovatie. Gesloten innovatie past beter bij de Koude Oorlog waarbij de overheid een monopolie positie heeft ten aanzien van de gebruikte techniek (kernwapens, tanks, etc.). In de cyberwereld heeft de overheid die technische monopoliepositie niet meer.

Daarnaast betekent open innoveren niet dat alle informatie frank en vrij wordt gegeven. De 'duty to share' hoeft niet in alle gevallen te worden opgevolgd. Open innovatie is geen heilig voorschrift maar de inlichtingendiensten zullen per geval moeten bekijken hoe open men kan optreden en herkennen wanneer open innovatie een kans van slagen heeft. Bijvoorbeeld, het project Symbolon waarbij de AIVD en MIVD samenwerken op gemeenschappelijke verwerking van SIGINT (Signal Intelligence) leent zich vanwege de specifieke domeinkennis niet voor open innovatie. Overigens heeft de politie al enige ervaring opgedaan met open innovatie zoals bij de ontwikkeling van het IRN (Internet Recherche Netwerk)

De inlichtingendiensten kunnen in navolging van het IRN gebruik maken van de principes van open innovatie om haar innovatievermogen te vergroten al heeft men in verhouding tot commerciële organisaties minder ruimte daartoe. De inlichtingendiensten moeten als het ware open gaan innoveren in een gesloten omgeving. Schematisch ziet er dit als volgt uit.



Voorheen vond innovatie voornamelijk gesloten plaats in een gesloten omgeving. De open innovatie beweging houdt een verschuiving van linksonder naar rechtsboven in. Omdat de omgeving open wordt dient de wijze van innoveren zich aan te passen. Voor de inlichtingendiensten betekent dat vooralsnog een verschuiving van linksonder naar linksboven. Een volledige verschuiving naar rechtsboven zal een brug te ver zijn maar hoeft ook helemaal niet nodig te zijn omdat per innovatievraag of –probleem vastgesteld moet worden hoe open of gesloten men moet innoveren. Wel is het zo dat er meer mogelijkheden zijn om de gesloten wijze van innoveren los te laten en meer samenwerking te zoeken met andere partijen. In de praktijk komen overigens ook mengvormen voor tussen open en gesloten innovatie. De hierboven genoemde Senseo mag dan wel ontwikkeld zijn tussen twee partijen (Philips en Sara Lee) die open stonden voor elkaar, maar aangezien andere partijen werden uitgesloten heeft dit samenwerkingsverband duidelijk gesloten trekken.

Om deze transitie te kunnen maken zal bij de inlichtingendiensten op de volgende punten verandering moeten komen:

- een organisatiecultuur die meer is ingesteld op ondernemerschap waarbij het nemen van risico's niet bij voorbaat wordt beperkt;
- een breder begrip hanteren van innovatie dan slechts incrementele verbeteringen;
- accepteren dat bij kennisverwerving ten behoeve van innovatie kennis kan weglekken ("you win some, you lose some").

Tot slot: open innovatie moet voor de inlichtingendiensten geen doel op zich zijn maar een middel om haar innovatievermogen te verbeteren. Door open innovatie kunnen de inlichtingendiensten volwaardig deel gaan uitmaken van diverse (kennis-) netwerken en daarmee ook aantrekkelijk blijven voor nieuwe medewerkers.

*Figuur 1: Verschillende relaties tussen open en gesloten innovatieprocessen en een open en gesloten omgeving.*

drs. Roelof Muis,  
teamleider Open Source INTelligence,  
Landelijke Eenheid, Nationale Politie

# Bedreigingen via internet

Het is maandagavond. Om 22.00 uur staat de laatste KNVB-zaalvoetbalwedstrijd van het seizoen gepland. Twee rivalen strijden om de eerste plaats. Het is een pittig duel waarbij een van de keepers herhaaldelijk wordt belaagd. Na de vierde lichamelijke confrontatie vallen de keeper en de spits van de tegenpartij over elkaar heen. De keeper bijt de spits toe: “de volgende keer schop ik je kop van je romp, lamxxx!” Het komt die wedstrijd nog een aantal keren tot hoogoplopende verwensingen. Na het eindsignaal bedanken de teams elkaar en schudden de beide kemphanen elkaar de hand.

### Het langetermijngeheugen van internet

De hierboven beschreven verwensingen in de fysieke wereld verschillen eigenlijk niet erg van de verwensingen op internet, maar met het grote verschil dat de digitale uitingen niet vervluchtigen en publiekelijk zichtbaar blijven. Recent is PvdA-voorzitter Hans Spekman een persoonlijke campagne gestart tegen dit soort online bedreigen, waarbij hij enkele voorbeelden van bedreigingen op zijn Facebookpagina publiceerde. De teksten liegen er niet om en hij is niet de enige die dit overkomt.

### Bedreigingen via internet

De aantallen bedreigingen via internet lopen in de duizenden per dag. Het team Open Source INTelligence (OSINT) bij de politie werkt aan een aanpak tegen deze vorm van bedreigingen. De afdeling is onder meer verantwoordelijk voor internetmonitoring op dreigingen binnen het rijkso domein en neemt deze taak zeer serieus. Elke dreiging op bijvoorbeeld bewindslieden of tijdens nationale evenementen is feitelijk een gevaar voor de democratische rechtsorde. Beslissingen binnen de maatschappij kunnen hierdoor beïnvloed worden. De Zembla-reportage over ‘bedreigde bestuurders’ is hiervan een realistisch voorbeeld.

### Strafbare bedreigen

Niet alle bedreigingen zijn strafbaar, maar er kan wel degelijk dreiging van uitgaan. Het aantal aangiftes is echter zeer laag en er komen nog minder ‘auteurs’ ter rechtzitting. Als de politie en het Openbaar

Ministerie alle (strafbare) bedreigingen zouden onderzoeken en vervolgen, zou daar vermoedelijk alle beschikbare capaciteit voor nodig zijn. Vanwege het volume van de bedreigingen is er behoefte aan een effectievere dreigingsduiding en een gerichtere aanpak jegens de auteurs. Dus efficiënter onderkennen, kwantificeren en kwalificeren waardoor politie-inzet op dreigingen geminimaliseerd kan worden.

### Innoveren

In samenwerking met het Ministerie van Veiligheid en Justitie, het Centre for Language and Speech Technology van de Radboud Universiteit Nijmegen en Tardis

Research is een dreigtweetmonitor in ontwikkeling op basis van een linguïstische studie van bedreigingen via internet. De dreigtweetmonitor filtert specifieke dreigingen door middel van zoekvragen. Dreigtweets worden naar ernst gerangschikt, waarna handmatig bestudering van de context plaatsvindt om uiteindelijk de serieuze (strafbare) dreigtweets te duiden. En resultaten uit het verleden bieden zeker garantie voor de toekomst. Zo troffen wij diverse verwijzingen naar ‘waxinelichtjeshouders’ aan. Tja, mensen zijn creatief, maar scherp blijven is belangrijk. Tijdens de eerste monitoringstest tijdens Prinsjesdag 2012, zijn in negen uur vijftien serieuze en specifieke dreigingen waargenomen en binnen de organisatie in het reguliere werkproces opgepakt. Een ‘serieuze dreiging’ kan bedoeld zijn als grap of andersom. Dat hangt af van de context en dus van de beoordeling. De huidige samenwerking tussen overheid, wetenschap en commercie binnen de ontwikkeling van de dreigtweetmonitor, kan daarbij zeer goed helpen.



# Digitaal bewijs onder de motorkap

A.A.W. Hijmering,  
diensthoofd EXO,  
Politie Rotterdam-Rijnmond

Het CrashCube project is een innovatieproject gestart vanuit een operationele behoefte binnen het domein van verkeersongeval analyse. In november 2010 startte Politie Rotterdam-Rijnmond met ondersteuning van het Nederlands Forensisch Instituut, de Rijksdienst voor het Wegverkeer en Rijkswaterstaat het project door middel van een ICT impuls vanuit het Ministerie van Justitie en Veiligheid. Het project is geïnitieerd om forensisch gevalideerde automotieve tools te ontwikkelen waarmee op een eenvoudige wijze data uit auto's gelezen worden.

Moderne auto's zitten vol met elektronica. Deze vooruitgang in de autotechniek leidt ertoe dat veel informatie besloten ligt in de elektronische chips van voertuigen. Autofabrikanten en monteurs gebruiken deze data om gebreken in het voertuig te detecteren. De data is versnipperd opgeslagen, wat betekent dat een variëteit aan protocollen nodig is om de data te kunnen uitlezen.

## CrashCube Tool

De elektronische onderdelen in auto's slaan storingen op die ontstaan tijdens een ongeval. De storingen bevatten tevens informatie over de omstandigheden waaronder de storing plaatsvindt, de zogenaamde freeze frames. Deze freeze frames kunnen informatie bevatten over bijvoorbeeld de kilometerstand, datum/tijdstip en snelheid tijdens de storing. De CrashCube is ontwikkeld om deze *freeze frames* uit te lezen. De data kan gebruikt worden om een beter beeld te geven van de omstandigheden waaronder het ongeval plaats vond. De CrashCube is daarmee een doorbraak voor verkeersongeval analyse.

Het gebruik van de tool draagt bij aan een optimale waarheidsvinding hetgeen het goed informeren van slachtoffers en/of nabestaanden onder andere met betrekking tot de schuldvraag mogelijk maakt.

## VINCube Tool

Elk motorvoertuig is voorzien van een chassis nummer/ Vehicle Identification Number [VIN]. Dit is een uniek toegewezen nummer, waarmee een auto geïdentificeerd kan worden. De meeste elektronisch aangestuurde onderdelen in auto's worden vanuit de fabriek eveneens voorzien van deze VIN. Een grote uitdaging bij de aanpak van auto-diefstallen is om een gestolen auto te herkennen. Criminelen veranderen de identiteit van de auto of verkopen die in onderdelen. De VINCube leest alle aanwezige elektronische VIN's uit. Door deze te checken in gestolen voertuig databases, is eenvoudig na te gaan of een betreffende auto gestolen

is, of gestolen onderdelen bevat. De VINCube draagt bij aan het bestrijden van voertuig-criminaliteit door middel van een zeer snelle en breed toepasbare controle op gestolen auto's of onderdelen. Het ultieme doel is het helen van auto's zo onaantrekkelijk mogelijk te maken, zodat ook het stelen niet meer rendabel is.

## Project resultaten

Het CrashCube project heeft een unieke kennispositie verworven omtrent de analyse van voertuigdata in relatie tot forensisch onderzoek. Deze kennispositie wordt door de politiek, het bedrijfsleven, de wetenschap en de politie, erkend en gesteund. Zo is ervaren dat diverse buitenlandse politiekorpsen kampen met problemen van dezelfde aard; een Europese aanpak kan een substantiële bijdrage leveren aan grensoverschrijdende criminaliteit. Gedurende het project zijn er twee volledig operationele tools ontwikkeld, die momenteel toegepast worden in de operatiën. Een adequate uitrol en borging van de technologie is nodig om niet achter te raken op de snelle ontwikkelingen in de industrie en een goede ondersteuning te bieden aan de gebruikers.

We hebben ervaren dat de projectresultaten niet eenvoudig weg te zetten zijn binnen de huidige beleidsstructuren, aangepast beleid is noodzakelijk. Met de komst van een Nationale Politie is er een nieuw uitgangspunt ontstaan voor de borging van de projectresultaten, ditmaal met een nationale focus. Deze structuur kan in de toekomst dienen als voorbeeld voor de uitrol van nieuwe projecten.



Wim van Geloven en Gunnar Bakker,  
NFI Academy, Nederlands Forensisch Instituut

Jaarlijks besteden we vele miljoenen aan innovatie. Ook in onze veiligheidssector reserveren we hiervoor budgetten en zijn er talloze programma's waarop projectvoorstellen worden ingediend. Toch bestaat vaak op zijn minst ongemak over het behaalde resultaat. Innovaties halen de eindstreep niet om reden van een gebrek of juist te veel aan creativiteit of te weinig focus en of aandacht. Ook zijn de keuzes waarop we zijn begonnen vaak niet helder te benoemen: soms op basis van gevoel, voorkeuren van management of me-too gedrag. De vraag is hoe we in onze sector het rendement van die innovatie zo hoog mogelijk kunnen krijgen. De inhoud van de innovatie (het wat) zou daarin wel eens minder aandacht hoeven krijgen dan de omgeving (het hoe en waarom).

# Hoe en waarom je innoveert is belangrijker dan wat je innoveert

De vaak gehoorde stelling dat innovatie het succes van de onderneming bepaalt is ook in onze sector waar, maar is nog niet zo eenvoudig. Apple is de nummer 1 in innovatiekapitalisatie. Het bedrijf is er in geslaagd om het rendement van de innovatie ver boven de 100% te laten uitstijgen. Die formule valt niet eenvoudig te kopiëren. Niet alleen de overheid maar ook het bedrijfsleven worstelt met dit onderwerp. Het leidt daarbij wel eens tot herhaling van op elkaar volgende tegengestelde reflexen. Het gevoel van te weinig vooruitgang wordt omgezet tot een subsidiereflex zonder goed na te denken wat we van de toekomst verwachten en met de nieuwe initiatieven willen bereiken. Het resultaat is teleurstelling en het stoppen van de innovatieprojecten zonder de reflectie waarom het resultaat er zo uit kwam te zien.

Nota bene, innovatie is per definitie het omgaan met mislukkingen. Als je iets probeert is er een kans dat het ook zal falen. Dat antwoord is niet van tevoren te geven, zeker niet per project afzonderlijk bekeken. Kunst is dus om die randvoorwaarden te

creëren waarbij het rendement van het hele portfolio wordt geoptimaliseerd. Dat begint al bij de wijze waarop we de voorwaarden voor innovatieprojecten creëren. Veel van de programma's zijn gebonden aan budgetrondes, tijdssloten, stringente regels, risicomijding of grote ideeën. Vanuit de stelling dat creativiteit maakbaar is, levert dat altijd een plan op: maar ook resultaat? Continue aandacht voor innovatie, met heldere spelregels en bijsturing van dag tot dag – stoppen is ook een optie - vormen sleutels voor succesvolle innovaties.

Daarnaast zou er bij het opstellen van innovatieplannen de afweging gemaakt kunnen worden tussen technologische en proces innovatie. Technologische innovaties krijgen vaak de meeste aandacht. Dat is concreet en kunnen we vastpakken. Proces innovatie levert net zulke resultaten op. Apple veranderde de aanblik van de muziekindustrie met een verbeterde mp3 speler. Om de effectiviteit van onderzoekers te verbeteren op een plaats delict gebruiken we bij het NFI de lessons learned in human factors bij het opleiden van piloten. Met

technieken uit de game sector vergroten we de forensic awareness bij brandweer en ambulancemedewerkers. We sturen echter voornamelijk impliciet op dit type projecten.

Het laatste aandachtspunt is de juiste balans tussen creativiteit en kapitalisatie. Voor innovatie is ontegenzeggelijk veel creativiteit en doorzettingsvermogen nodig. Zonder kapitalisatie krijgt dat idee geen waarde. Een oplossing hiervoor is het richten van de projecten op het oplossen van reële problemen en bij gebleken geschiktheid pas op te houden na een succesvolle toepassing. Niet te vroeg juichen dus.

Als we kritisch kijken naar de omgeving waarin innovaties vorm krijgen, is de wijze waarop we dat doen nog te innoveren. De uitdagingen waar we als veiligheidssector voor staan en het tijdsgewricht vormen een extra impuls om het rendement van onze innovaties te verhogen. Met een goed innovatieklimaat vangen we nog niet direct meer boeven maar zorgt er voor dat we dat in de toekomst veel beter kunnen doen.



# Onzekere toekomst in de Nationale Risicobeoordeling (NRB)

Wat zou de toekomst op het terrein van veiligheid in petto kunnen hebben? Dat is voor beleidsmakers een cruciale vraag. Daarom doen we in Nederland aan 'nationale risicobeoordeling'. De toekomst is echter open. Voorspellen is een illusie. Hoe wordt in de Nationale Risicobeoordeling met onzekere toekomst omgegaan? Wat kan er beter?

## De Nationale Risicobeoordeling (NRB): een toekomstgerichte best practice

"Welke bedreigingen van de nationale veiligheid zouden tot maatschappelijke ontwrichting kunnen leiden" is de centrale vraag in de Nationale Risicobeoordeling (NRB), die sinds 2007 elk jaar wordt geproduceerd. Hoewel de bedreigingen in klassieke risicotermen (kans en effect) worden 'beoordeeld', is de NRB een vernieuwende manier om na te denken over onzekere toekomst. Het is geen inventarisatie van risico's die zich in het verleden al voldoende hebben gemanifesteerd om met behulp van statistiek te kunnen worden ingeschat. Integendeel. Op een (inmiddels flink) aantal veiligheidsthema's worden scenario's ontwikkeld waarin denkbare, doch ongewenste, toekomst worden doordacht, die vervolgens beoordeeld worden door experts<sup>1</sup>. Die scenarioverzameling wordt gebruikt om risico's te vergelijken en te prioriteren. Dat is bedoeld als input voor een brede en nuchtere afweging. De NRB wordt gebruikt om capaciteiten te benoemen die nodig zijn om maatschappelijke ontwrichting aan te kunnen.

De NRB is dus een toekomstgerichte analyse van mogelijke bedreigingen van de nationale veiligheid. Dat is een stap vooruit. Het is niet voor niets dat de OESO (2009, 22) de NRB (samen met de Britse National Risk Assessment) kwalificeert als best practice. De centrale rol van scenario's in de NRB is vernieuwend. In het algemeen is de belangstelling voor toekomstverkenning onder risico-experts minimaal, ondanks dat

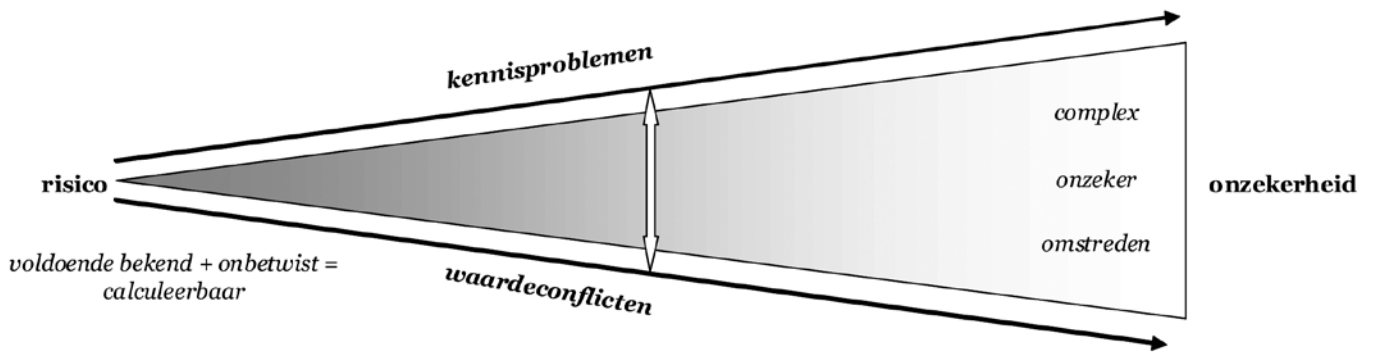
door sommigen wel erkend wordt dat risicobeoordeling het inventariseren van scenario's behelst, en dat risicobeoordeling impliciet doch onvermijdelijk uitmondt in een scenariobenadering (Van Asselt e.a. 2010, 18).

## Doorontwikkelen tot onzekerheidsarrangement

Toch hinkt de NRB op twee gedachten, waardoor mensen op het verkeerde been worden gezet. Zo stelde de WRR (2011) in een reflectie op de NRB dat "alle veiligheidsvraagstukken worden behandeld als voldoende bekend en onbetwist" (p. 42). Dat is een onjuiste lezing. De NRB draait juist om de vraag wat er in de toekomst mogelijk zou kunnen zijn. Het interpreteren van onzekerheid staat centraal. Tegelijkertijd is het wel waar dat "kennisproblemen en waardeconflicten (...) aan het zicht [worden] onttrokken" (p. 42). De NRB zet niet in de etalage dat het een poging is om met behulp van toekomstverkenning relevante onzekerheden te onderzoeken en er grondig over te discussiëren. In de uiteindelijke presentatie is de onzekerheid onzichtbaar. Dat is volgens ons een gemiste kans.

Met hetzelfde materiaal zijn andere dingen te doen. Wat neergezet wordt als waarschijnlijkheid en impact zijn geen harde feiten, maar gemiddelden van uiteenlopende inschattingen van experts. De variatie in die inschattingen geeft inzicht in de mate van onzekerheid over die risico's. In de eerste jaren werd aan die variatie vrijwel voorbij gegaan. Sinds 2011 wordt de bandbreedte in expertopvattingen wel opgenomen in een bijlage van

<sup>1</sup> De NRB 2012 scenario's zijn recentelijk afgerond. Het eindrapport waarin de scenario's afzonderlijk en in vergelijkend perspectief worden beschreven zit in de pijplijn (*Nieuwsbrief Analistennetwerk Nationale Veiligheid*, januari 2013).



Figuur 1 (bron: WRR 2011)

de Bevindingenrapportage. Een heel voorzichtig stapje in de goede richting. Onzekerheidsacceptatie betekent het aanvaarden van kennisproblemen en waardeconflicten en het actief uitdragen daarvan in houding en gedrag. Er is behoefte aan onzekerheidsarrangementen, dat wil zeggen aan georganiseerde manieren voor reflectie, onderzoek en dialoog (WRR, 2011). De NRB heeft de potentie van een wezenlijk interdepartementaal onzekerheidsarrangement. Dat vergt wel dat in de NRB niet alleen gekeken wordt naar verschillende risico's, maar ook naar het verschil in risico's.

#### Aandacht voor onzekerheid

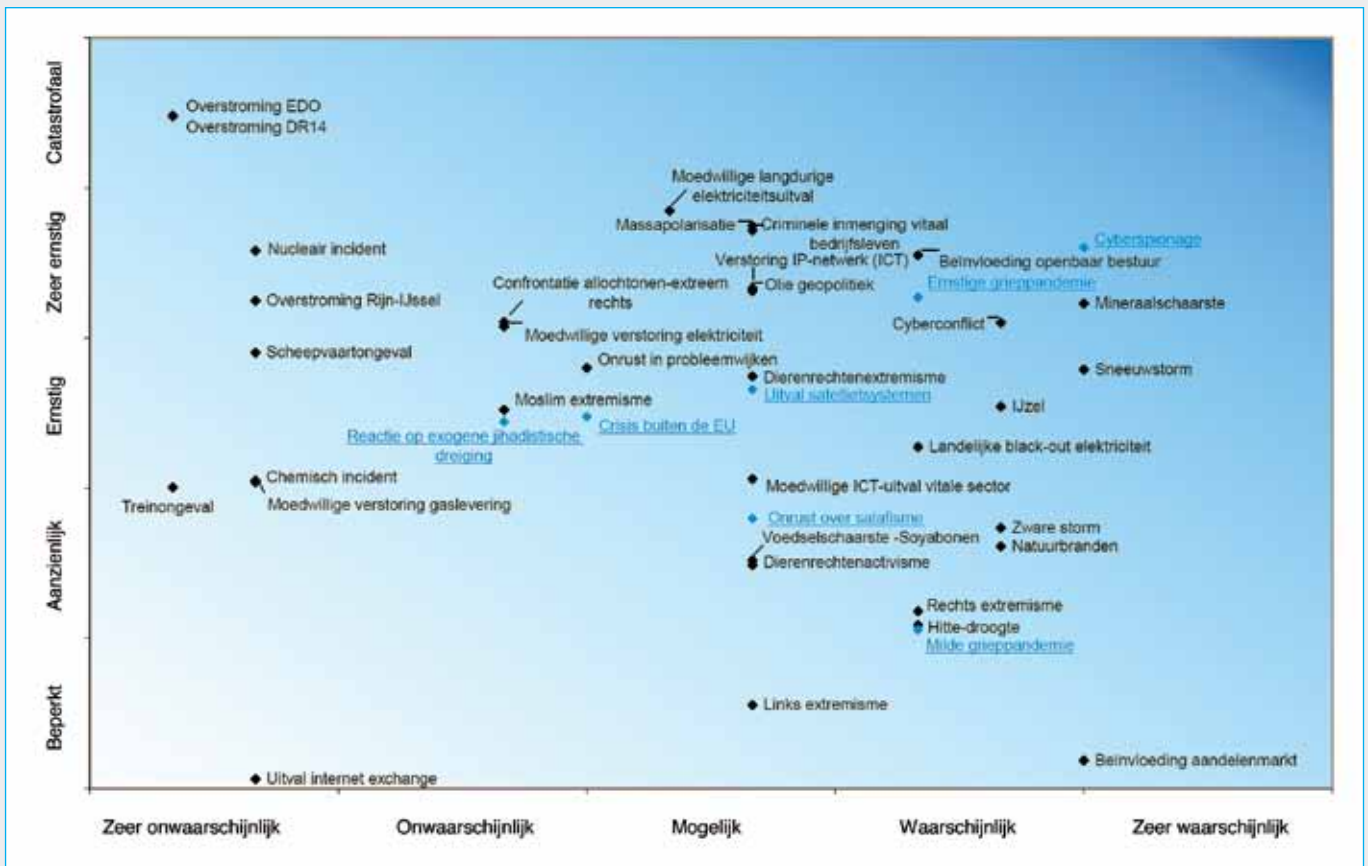
Niet alle risico's zijn even goed bekend en ook over de ernst zijn er meningsverschillen (figuur 1). Als er veel kennisproblemen of waardeconflicten rondom een bepaald risico bestaan, is er sprake van onzekerheid. Het zou een stap vooruit zijn als in de NRB erkend wordt dat risico's verschillen in de mate van onzekerheid. De griepandemie is een voorbeeld van een risico waar men over relatief veel informatie beschikt. Er kan gebruik gemaakt worden van casuïstiek, o.a. drie redelijk recente pandemieën zoals SARS, om toekomstige bedreigingen en de mate van maatschappelijke ontwrichting in te schatten. In de NRB2011 zijn de onzekerheidsmarges van de pandemiescenario's minder groot dan bij andere scenario's. Het scenario van de uitval van satellietssystemen door te grote zonneactiviteit is met veel meer onzekerheid omgeven. Zoiets heeft nog nooit eerder plaatsgevonden. Er kan dus niet voortgebouwd worden op ervaringen uit het verleden. Het is een denkbare, maar onbekende bedreiging van de nationale veiligheid. De verkenning van deze onzekere toekomst is dus veel meer oriënterend. De variatie in de inschatting van wat er mogelijk zou kunnen gebeuren en wat voor impact dit zal hebben op de samenleving is in de NRB2011 groter dan bij de pandemiescenario's. In de NRB worden meer bekende en onzekere risico's meegenomen, maar zulke verschillen in risico's zijn nauwelijks te achterhalen.

Onbekend maakt meestal onbemind, maar de NRB bewijst juist dat het goed mogelijk is om onbekende bedreigingen van de nationale veiligheid in de afweging

te betrekken. In de communicatie over de NRB staat echter het risicodiagram centraal waarin zowel de ingeschatte impact als de relatieve waarschijnlijkheid van een scenario worden weergegeven (figuur 2). Alle onderzochte scenario's worden daarin geplaatst. Deze presentatie suggereert een bepaalde hardheid van de inschattingen, die geen recht doet aan het onderliggende proces en aan de onzekerheid van de toekomst die worden beoordeeld. Die informatie over onzekerheid is echter beleidsrelevant. Voor een relatief bekend risico kan bijvoorbeeld specifiek preventief beleid worden gemaakt, terwijl voor een onzeker risico het versterken van meer algemene capaciteiten mogelijk verstandiger is.

Het risicodiagram suggereert dat alleen risico's die een hoog gemiddelde hebben op waarschijnlijkheid en impact beleidsmatige aandacht behoeven. Door





Figuur 2: Risicodiagram NRB 2011

te werken met gemiddelden valt echter weg dat bepaalde scenario's in feite heel onzeker zijn. Voor het nadenken over toekomstige ontzetting en de daarvoor benodigde capaciteiten zijn zulke scenario's juist heel belangrijk. Onzekerheid verdwijnt te gemakkelijk buiten beeld als zogenaamd onwaarschijnlijk, ongevaarlijk of onbelangrijk. En daarmee doet de NRB zichzelf te kort.

De kunst is om manieren te vinden om ook onzekerheid een zichtbare plek te geven in de NRB, bij voorkeur in of gecombineerd met het diagram dat zo gemakkelijk een eigen leven leidt. De bandbreedtes in de inschattingen zouden bijvoorbeeld in het diagram opgenomen kunnen worden. Of in een tweede diagram zouden op de ene as kennisproblemen in relatie tot een bepaald scenario kunnen worden weergegeven en langs de andere as de mate van waardeconflicten. Dan worden onzekerheden benoemd, wat beleidsmakers kan helpen bij het maken van genuanceerde risicovergelijkingen. En er zijn vast nog andere manieren te bedenken om onzekerheidsacceptatie vorm te geven. Met deze suggesties willen we vooral duidelijk maken dat met hetzelfde materiaal meer gedaan kan worden. Het gaat dus niet om het verder ontwikkelen van de methodiek. Er valt vooral veel te winnen in onzekerheidscommunicatie. Nu wordt om begrijpelijke redenen, maar wel ten onrechte, gesuggereerd dat de beoordeling van onzekere toekomst tot een eenduidige prioritering

leidt. Dat is comfortabel, maar deze insteek leidt er ook toe dat de NRB in de politiek-bestuurlijke gremia gemakkelijk tot een hamerstuk verwordt.

Door onzekerheid zichtbaar te maken wordt er meer ruimte gemaakt voor een politieke discussie. Het prioriteren en afwegen is uiteindelijk politiek en moet dat ook zijn. Vergelijkingen van potentiële bedreigingen, waarin de NRB op een innovatieve manier voorziet, zijn daarvoor nuttige input. De NRB is geen spijkerhard besliskader. Dat weet iedere bij de NRB betrokkene heel goed, maar de verleiding lijkt te groot om het toch als een 'speaking-truth-to-power' exercitie te presenteren. De NRB is er nog niet in geslaagd om input te zijn voor een politiek afwegingsproces. Maar er liggen wel kansen om stappen in die richting te zetten en het zou jammer zijn die te missen. Een internationale best practice verdient het om verbeterd en versterkt te worden.

#### Literatuur

- M.B.A. van Asselt, S.A. van 't Klooster, P.W.F. van Notten and L.A. Smits, *Foresight in action: Developing policy-oriented scenarios*, London: Earthscan, 2010.
- OECD, *Innovation in country risk management*, Paris 2009.
- WRR, *Evenwichtskunst: Over de verdeling van verantwoordelijkheid voor fysieke veiligheid*, Den Haag 2011.

Peter van Zanten,

senior managing consultant Berenschot; lid en secretaris commissie Onderzoek asbestvondst Kanaleneiland (Commissie Jansen)

Judith van Krieken,

consultant, Berenschot, ondersteuner Commissie Jansen

# Commissie Onderzoek asbestvondst Kanaleneiland

Op 4 december 2012 zijn de bevindingen van de Commissie Onderzoek asbestvondst Kanaleneiland gepresenteerd. Deze onafhankelijke commissie is ingesteld door het college van burgemeester en wethouders van de gemeente Utrecht, naar aanleiding van het asbestincident dat zich in juli 2012 voordeed in de Utrechtse wijk Kanaleneiland. De belangrijkste vraag van de commissie, en vele anderen, was: hoe heeft het asbestincident in Kanaleneiland zo groot kunnen worden?

### Wat is er gebeurd?

Vanaf maandag 16 juli 2012 wordt er in opdracht van woningcorporatie Mitros asbest verwijderd aan een flat in het Utrechtse Kanaleneiland. Op zondag 22 juli wordt groot alarm geslagen vanwege de vondst van asbest. Naar aanleiding van deze vondst, worden bewoners van meerdere flatgebouwen geëvacueerd, delen van de wijk afgesloten en schaalde de crisisorganisatie op tot GRIP 2. Op 3 augustus wordt afgeschaald. Het incident heeft veel media aandacht gekregen en veel onrust veroorzaakt bij bewoners. De verwachting is dat rond het verschijnen van dit artikel (ruim 6 maanden na dato) de laatste bewoners kunnen terugkeren naar hun woning.

### Bevindingen van de onderzoekscommissie

De commissie heeft bij haar onderzoek zowel de leden van de crisisbeheersingsorganisatie, de woningcorporatie, de asbestsaneerders als de bewoners van de wijk Kanaleneiland betrokken. Dit leverde een uitgebreide feitelijke reconstructie, 43 observaties (analyse), zes conclusies en vijf aanbevelingen op. De commissie heeft van zowel het college van B&W van Utrecht, alsmede van alle fracties in de gemeenteraad complimenten ontvangen voor de heldere en transparante rapportage. Ook de bewoners waren lovend over het werk van de commissie. Voor de bewoners van Kanaleneiland waren de uitkomsten van het onderzoek een belangrijke stap in de verwerking van de traumatische gebeurtenis die hen was overkomen. Veel bewoners waren door de gebeurtenissen het vertrouwen in de overheid en de woningcorporatie kwijt geraakt. Daarmee heeft het onderzoek tevens een verzoenend karakter gehad en bijgedragen aan het herstel van vertrouwen in de overheid.

Daarnaast is duidelijk geworden dat met de asbestsanering in Nederland grote belangen gemoeid zijn en dat bij het functioneren van, en toezicht op de asbestsaneringsbranche vraagtekens kunnen worden gezet.

In het onderzoeksrapport presenteert de commissie de volgende conclusies:

1. *De maatregelen die zijn getroffen naar aanleiding van de asbestvondst in Kanaleneiland zijn achteraf gezien disproportioneel.*

Bij de opschaling van de hulpdiensten na de eerste asbestvondsten was onvoldoende feitelijke informatie beschikbaar, waardoor hulpdiensten op eigen inzicht en uit voorzorg een groot gebied hebben afgezet en opschalden naar GRIP 2. Echter, de geconstateerde meetwaarden lagen onder de zogenaamde 'evacuatiernorm' en er bestonden zeer beperkte risico's voor de volksgezondheid. Vanuit voorzorg en de zorgplicht van zowel gemeente als de woningcorporatie, was het begrijpelijk dat alle flats ontruimd zijn, maar dit had geen spoedeisend en dwingend karakter hoeven hebben.

2. *De crisisorganisatie heeft onvoldoende gefunctioneerd en de genomen maatregelen waren onnodig belastend voor de bewoners.*

Twee zaken sprongen er voor de commissie uit: de crisiscommunicatie en de besluitvorming in het Gemeentelijk Beleids Team (GBT). De commissie constateert dat de crisiscommunicatie niet professioneel is opgepakt; de communicatiefunctie was bij zowel gemeente als woningcorporatie belegd, er waren te weinig mensen beschikbaar en communicatieboodschappen waren niet op elkaar afgestemd. Over de besluitvorming in het GBT oordeelt de commissie dat enkele besluiten van het GBT onnodig verwarring hebben gezaaid en burgers onnodig hebben belast. Met name het besluit om een noodbevel voor een deel van Kanaleneiland uit te vaardigen was volgens de commissie onnodig ingrijpend. Hierdoor werd de wijk in korte tijd hermetisch afgesloten en konden bewoners de wijk niet meer in of uit. Dit leverde o.a. gebroken gezinnen op en leidde tot veel onrust bij bewoners.



Foto: Bert Spiertz

*3. De reactie van de crisisorganisatie op de ontstane onrust bij bewoners was onvoldoende.*

Het perspectief van de bewoners van Kanaleneiland heeft niet centraal gestaan. De commissie constateert dat de onrust en beleving van bewoners door de crisisorganisatie als bijzaak en een 'lastige bijkomstigheid' werden gezien. De crisisorganisatie lijkt zich onvoldoende bewust geweest van de impact van acties op burgers, zoals het plotseling verschijnen van 'mannen in witte pakken', het afsluiten van de wijk en de plotselinge evacuatie.

*4. Over de asbestsanering is niet gecommuniceerd, de asbestsanering is onjuist uitgevoerd en het toezicht op de asbestsanering heeft niet gefunctioneerd.*

De asbestsaneringsbranche is een zeer complex georganiseerde sector. Het toezicht op asbestsanering wordt grotendeels vanuit de private sector gehouden. De commissie concludeert dat de asbestsanering ondeugdelijk is uitgevoerd en dat het toezicht hierop niet adequaat was. Ook hadden burgers voorafgaand aan de asbestsanering goed geïnformeerd moeten worden over de werkzaamheden en de gevolgen ervan

voor het dagelijks leven (bijvoorbeeld geen balkons betreden en ramen en deuren gesloten houden). Dit is niet gebeurd. Bewoners verkeerden in onwetendheid en hebben onbewust risicovol gedrag vertoond, wat achteraf de onrust en woede heeft vergroot.

*5. Asbest roept bij burgers angstige gevoelens op, wat vraagt om op diverse doelgroepen afgestemde informatievoorziening en communicatie.*

Asbest roept onrust en angst op, maar bij het brede publiek is weinig bekend over de feitelijke risico's van asbest voor de volksgezondheid. Het is lastig om goed over gezondheidsrisico's te communiceren, of deze nu groot of beperkt zijn, en de angst en onzekerheid bij burgers helpen niet om risico's in de juiste proporties te bezien en te accepteren. In geval van maatschappelijke onrust (zoals het geval was in deze casus) bestaat er een verschil tussen de gepercipieerde dreiging en de feitelijke dreiging. Communicatie moet hier rekening mee houden.

*6. Als dit incident een voorbeeld is van de ontwikkelingen in de komende periode met betrekking tot asbestsanering, dan ligt hier een taak voor de Rijksoverheid om te beoordelen of de wijze van zelfregulering door de branche met marginaal toezicht vanuit de overheid, voldoet.*

De komende jaren zullen op grote schaal asbestsaneringen plaatsvinden, onder andere in scholen en in de sociale huursector. Zoals reeds geconcludeerd, is de asbestsaneringsbranche complex georganiseerd en is de asbestsanering in Kanaleneiland niet veilig uitgevoerd. Indien dit wordt doorgetrokken naar toekomstige saneringsoperaties, is het wachten op het volgende incident à la 'Kanaleneiland'. Hierbij spelen grote sociale (maatschappelijke onrust) en financiële belangen mee (de ingeschatte kosten van een reguliere sanering van de sociale huursector bedraagt € 3,8 miljard). De commissie concludeert dan ook dat de Rijksoverheid opnieuw moet beoordelen of de wijze van zelfregulering van de asbestbranche en het marginale centrale toezicht erop, nog voldoende.

**Tot slot**

De commissie is zich ervan bewust dat veel activiteiten 'geruisloos' goed zijn verlopen en dat er in mindere mate aandacht is besteed aan deze activiteiten die tot resultaten hebben geleid door de inzet, expertise en betrokkenheid van medewerkers. Bij het onderzoek heeft de commissie geconstateerd dat medewerkers van de crisisorganisatie een grote inspanning hebben geleverd en dat de crisisorganisatie tot het uiterste is belast.

Het volledige rapport met bijlagen is te downloaden van de website van de gemeente Utrecht <http://www.utrecht.nl/smartsite.dws?id=381529>

Menno van Duin,

lector Crisisbeheersing (Nederlands Instituut Fysieke Veiligheid/

Politieacademie) en bijzonder lector Regie van Veiligheid

(Hogeschool Utrecht i.s.m. de Veiligheidsregio Utrecht)

# De asbestcrisis in Utrecht: over **evalueren en oordelen**<sup>1</sup>

## Inleiding

Begin december kwamen twee rapporten uit over de asbest-crisis<sup>2</sup> in Kanaleneiland. Ten eerste het rapport van de onderzoekscommissie onder leiding van de heer Jansen (oud CdK Overijssel; verder verwezen als commissie Jansen) dat in opdracht van het college van B&W van de gemeente Utrecht is opgesteld en een rapport van het COT, dat in opdracht van woningbouwcorporatie Mitros is geschreven. Inmiddels heeft ook het verantwoordingsproces in de Utrechtse gemeenteraad (13 december 2012) plaatsgevonden waarmee het thans een geschikt moment lijkt om de balans op te maken.

In deze bijdrage zullen eerst kort de conclusies van beide rapporten worden weergegeven waarna wat langer zal worden stil gestaan bij de waarde en bijdrage van beide rapporten. Mijn conclusie na lezing van beide rapporten en het verslag van de gemeenteraad daarover is duidelijk. Het leidt geen twijfel dat er in Utrecht (als we de evaluatoren moeten geloven zelfs forse) fouten zijn gemaakt na metingen van asbest in verschillende woningen; door de gemeente, de organisaties die de crisis bestreden en door woningbouwcorporatie Mitros. Toch draagt de manier van rapporteren en concluderen maar in beperkte mate bij aan het doorgronden van de problemen en moet de vraag gesteld worden of wij in de toekomst moeten doorgaan met het doen van evaluaties op dergelijke (gescheiden) wijze. Evaluatoren zijn over het algemeen veel te veel gericht op oordelen en soms ook veroordelen, en veel te weinig op het begrijpen.

De twee evaluaties doen op verschillende plaatsen te weinig recht aan de weerbarstigheden en uniciteit van crises. Daarmee is er onvoldoende gevoel voor de manieren waarop crises zich kunnen ontwikkelen en voor de dilemma's waarmee men in dergelijke situaties

geconfronteerd wordt. Waarom ging het nu zoals als het ging en wat zou in een dergelijke situatie verwacht mogen worden?

In twee afzonderlijke kaders zijn de belangrijkste conclusies van beide rapporten weergegeven. Uiteraard kennen dergelijke korte statements altijd beperkingen en worden er vaak in de toelichtende teksten nuances aangebracht. Tegelijkertijd zijn het juist deze conclusies die de media halen en centraal staan in de opgestelde persberichten. Bij veel van de evaluaties zijn het ook juist deze kernachtige zinnen die binnen de onderzoekscommissie zelf de meeste aandacht krijgen en langdurig bediscussieerd worden.

### Commissie Jansen

1. De maatregelen die zijn getroffen naar aanleiding van de asbestvondst in Kanaleneiland zijn achteraf disproportioneel.
2. De crisisorganisatie heeft onvoldoende gefunctioneerd en de genomen maatregelen waren onnodig belastend voor de bewoners.
3. De reactie van de crisisorganisatie op de ontstane onrust bij bewoners was onvoldoende.
4. Over de asbestsanering is niet gecommuniceerd, de asbestsanering is onjuist uitgevoerd en het toezicht op de asbestsanering heeft niet gefunctioneerd.
5. Asbest roept bij burgers gevoelens op, wat vraagt om op diverse doelgroepen afgestemde informatievoorziening en communicatie.
6. Als dit incident een voorbeeld is van de ontwikkelingen in de komende periode met betrekking tot asbestsanering, dan ligt hier een taak voor de Rijksoverheid om te beoordelen of de wijze van zelfregulering door de branche met marginaal toezicht vanuit de overheid, voldoet.

<sup>1</sup> Bij de totstandkoming van dit artikel heb ik dankbaar gebruik gemaakt van zowel de commentaren vanuit de redactie als van Vina Wijkhuijs.

<sup>2</sup> Volgens de wet wordt een dergelijke situatie misschien geen crisis genoemd; in meer wetenschappelijke termen zeker wel: een situatie van collectieve stress gekenmerkt door dreiging, urgentie en onzekerheid.

#### COT

1. Mitros had ruime aandacht voor asbest in de voorfase; wel zijn er verbeterpunten.
2. Mitros heeft zich intensief ingespannen om de calamiteit adequaat af te handelen; dit was deels wel en deels niet effectief.
3. De focus lag op het handelen uit voorzorg; de impact van maatregelen bleef onderbelicht.
4. Er zat een onbalans tussen de werkelijke risico's en de uitstraling en beleving van maatregelen.
5. De publieks- en bewonerscommunicatie verliepen niet goed genoeg; de opgelopen achterstand is niet meer ingelopen.

#### Een andere perceptie op conclusies

De eerste conclusie van de commissie Jansen is dat de genomen maatregelen disproportioneel zijn. Daaraan wordt toegevoegd dat de genomen maatregelen onnodig belastend waren voor de bewoners (conclusie 2). Daarmee geeft de commissie een zeer stevig statement af. In de toelichting relativeert men het wel ten dele, maar de stevige, en mijns inziens onjuiste, conclusie staat apart gedrukt. In de media zijn het vooral ook deze zinnen die geciteerd zijn om het Utrechtse falen weer te geven. Zo werkt dat nu eenmaal. Een op zich genuanceerd rapport krijgt door scherpe conclusies een andere lading.

Het is goed om te proberen te verklaren waarom er gehandeld is zoals er is gehandeld (de maatregelen die genomen zijn) en vervolgens daar - voor zover dat nodig wordt gevonden (van mij hoeft dat niet) - conclusies aan te verbinden en aan te geven of hier sprake is van disproportionaliteit. De commissie Jansen volgt deze logica maar zeer ten dele. De commissie constateert dat op basis van onvolledige informatie zondag 22 juli 2012 een evacuatie is gestart die geen spoedeisend karakter had. Hoewel de commissie zich kan voorstellen dat de gemeente het zekere voor het onzekere heeft genomen (voorzorgprincipe), is de commissie van mening dat een en ander rustiger en meer gefaseerd had moeten geschieden.

Als wij de beide rapporten en datgene wat in het gemeentelijk debat gezegd is lezen, komen ten minste drie factoren naar voren die bij de eerste (blijkbaar disproportionele) maatregelen een rol speelden. Cruciaal is de start van de gehele operatie waarover de commissie Jansen en het COT het een en ander zeggen. Zondagochtend 22 juli uur wordt de directie van Mitros in kennis gesteld door de behandelend medewerker van Mitros dat er asbestbesmetting is geconstateerd.

Inmiddels zijn vijf woningen ontruimd en is er ook elders asbest gevonden. Mitros belt conform het eigen asbestprotocol de piketdienst van de afdeling Vergunningverlening, toezicht en handhaving (VTH) van de gemeente Utrecht en doet rond 11 uur melding van de situatie. De betreffende gemeentelijk ambtenaar is op dat moment telefonisch al in gesprek en kan dientengevolge niet het telefoonnummer van de piketdienst openbare orde en veiligheid (OOV) opzoeken. Hij adviseert de medewerker van Mitros de meldkamer te bellen (112) en daar het juiste nummer op te vragen.<sup>3</sup> Mitros belt om 11.48 uur het alarmnummer 112 en daarop worden de hulpdiensten door de meldkamer gealarmeerd. (...) De meldkamer laat leidinggevend van brandweer, politie en ambulance-diensten ter plaatse gaan ..." (Cie-Jansen, p. 20).

In het raadsdebat van 13 december 2012 is - op verzoek van een raadslid - een (letterlijke) weergave van het gesprek van de Mitros-medewerker gegeven:

*"Ik zit met een asbestcalamiteit. (...) De gehele omgeving is nu ook al besmet. Vervolgens vraagt de meldkamer waar het is: "Het is aan de Stanleylaan". Daarna zegt de melder dat hij doorverbonden wil worden met het piket OOV. De meldkamer vraagt verder door. "Er zijn 48 woningen besmet met asbest". Achteraf blijkt dit onjuist te zijn. Hierop vraagt de meldkamer wat het acute gevaar is en dan zegt de melder: "Er zijn inmiddels vijf woningen uitgeplaatst en er moeten nog 43 bewoners uitgeplaatst worden". Het openbare terrein blijkt eveneens te zijn besmet met spuitasbest, "dat nog gevaarlijker is dan ander asbest". Vervolgens zegt de melder: "Het ligt op balkons, op vensterbanken op struiken en garageboxen en dus in de omgeving". De meldkamer vraagt of het is uitgewaaid: "Ja inderdaad, het is ook uitgewaaid. We hebben inmiddels uitslagen gekregen en nu blijkt ook de omgeving besmet".*

Het verbaast mij dat in geen van de evaluaties dit citaat is weergegeven, want juist dit geeft een zo heldere situatieschets. Er is sprake van een fors probleem. Asbest is immers een stof die tot de verbeelding spreekt en al snel 'alle stoppen doet doorslaan'. Als er al vijf huizen zijn ontruimd en er ook elders asbest is gevonden, kan het haast niet anders dan dat de betrokken diensten actief worden en maatregelen nemen om bewoners in veiligheid te brengen en verdere besmetting zo veel als mogelijk te voorkomen en te beperken. Het is volstrekt begrijpelijk dat de meldkamer op basis van dit bericht 'all out' gaat en er ter plaatse een COP1 wordt ingericht en grootschalig maatregelen worden genomen. Er is immers geen helder vastgelegd en vastgesteld asbestbeleid op grond waarvan de meldkamer als ware het een routinehandeling zou kunnen reageren.

<sup>3</sup> Verwijten door een PvdA-raadslid tijdens het debat dat Mitros geen 112 had moeten bellen, zijn dus onterecht. De gemeenteambtenaar had niet moeten doorverwijzen naar 112.



Foto: Bert Spiertz

Daarmee stuiten wij op een cruciaal dilemma: in hoeverre neem je op basis van beperkte informatie verstrekkende maatregelen (mensen uit huizen halen)? Is het te verdedigen om in deze acute situatie als hulporganisaties (en gemeente) af te wachten tot er meer en betere informatie aanwezig is, of kan op basis van eerste metingen die laag zijn worden uitgelegd dat er geen reden is tot snelle (en drastische) maatregelen? Natuurlijk is dat laatste mogelijk, maar welke hulpdiensten zullen na dergelijke berichten eerst met de armen over elkaar gaan zitten? Ook moet niet vergeten worden dat dergelijke meldingen zeer schaars zijn en er nauwelijks precedents bestaan. De hulpdiensten werken hier vanuit het principe 'het zekere voor het onzekere nemen', in plaats van eerst het zekere te willen weten.

Daarnaast doet zich het extreem lastige dilemma voor dat het vrijwel onmogelijk is om vanuit het (gezien de situatie dus begrijpelijke) voorzorgsbeginsel ('zekere voor het onzekere') maatregelen te nemen en tegelijkertijd te communiceren dat de situatie feitelijk niet ernstig is en de gezondheidsrisico's voor de bewoners zeer gering zijn. Het is niet uit te leggen dat de brandweer met beschermende kleding brieven bezorgt en maatregelen neemt, het afgezette gebied sterk wordt vergroot om de beveiliging en uitvoering beter mogelijk te maken, en tegelijkertijd gecommuniceerd wordt dat de problemen gering zijn. Tegenstrijdige boodschappen zijn niet uit te leggen.

Ik vind de maatregelen dus niet disproportioneel, want goed verklaarbaar. Ik ben er vrij zeker van dat in deze

situatie (met deze melding, het gebrek aan ervaring met vergelijkbare gevallen, de reeds geconstateerde besmettingen, de afwezigheid van een landelijke procedure, de gevoeligheden die rondom asbest leven en met het gebruik van het woord spuitasbest) vrijwel overal in Nederland op vergelijkbare wijze zou zijn gehandeld. Als de maatregelen begrijpelijk en verklaarbaar zijn, past het etiket 'disproportioneel' niet. Met de rust achteraf kunnen wij dergelijk handelen wel veroordelen; maar gezien de wijze waarop de 'crisis' startte en het gebrek aan ervaring en procedures kunnen wij een en ander ook op zijn minst begrijpen.

Opvallend is dat in het raadsdebat de raadsleden achter de kritische toon van het rapport van de commissie Jansen staan, maar tegelijkertijd wel aangeven het goed te kunnen begrijpen dat de gemeente zo handelde. "GroenLinks vindt het begrijpelijk dat de locoburgemeester op zondag 22 juli op basis van zeer beperkte informatie besloot het zekere voor het onzekere te nemen". Na een dag had de gemeente moeten 'terugschalen' omdat de risico's minder ernstig waren dan gedacht, zo wordt verschillende keren aangegeven. Dat lijkt achteraf zo simpel; mede omdat in de rapportage te weinig wordt uitgelegd wat de dilemma's waren en hoe lastig het in die constellatie is de koers 180 graden te wijzigen. Het COT-rapport slaagt er beter in enkele lastige thema's te duiden (p. 21-23).

Al met al kwamen in beide evaluaties de dilemma's onvoldoende uit de verf. Misschien heeft dat deels te maken met het feit dat niet één maar twee evaluaties gescheiden van elkaar plaatsvonden, waarbij vanuit verschillende achtergronden werd gewerkt en met verschillende respondenten werd gesproken. Op zich had men echter de dilemma's meer inzichtelijk kunnen maken, maar dan zouden wel dezelfde gebeurtenissen vanuit twee werelden moeten zijn belicht. Zo is het echter niet gedaan.

Belangrijke dilemma's waren onder andere, zo leert de casus:

- kan bij een objectief beperkt, maar subjectief totaal anders ingeschat risico (we hebben het over spuitasbest...) door verantwoordelijken wel gepast terughoudend (en niet vanuit voorzorg) worden geopereerd?
- hoe kan je zowel voorzorgsmaatregelen nemen en tegelijkertijd goed communiceren dat de situatie niet zo ernstig is (terwijl bijvoorbeeld de brandweer in witte pakken moet werken)?
- wie is nu primair 'in the lead' en wanneer krijgt of neemt een gemeente 'het aapje op zijn schouder'?
- wat maakt dat er met enige regelmaat over asbestproblemen wordt gerept, maar het aantal vastgestelde maatregelen, inclusief de communicatie richting publiek erover, zo beperkt is?



Tot zover over de inhoudelijke oordelen waarbij ik – gezien de omvang van dit stuk – vooral heb ingezoomd op die thema's die ook publiekelijk het meeste aandacht kregen. Met de observaties (wel erg veel: 43!) en de aanbevelingen van de commissie Jansen heb ik veel minder problemen. Het tweede thema betreft de vraag of wij dergelijke beoordelende evaluaties nog moeten wensen?

### Evalueren en oordelen

Door verschillende personen is in het verleden en recent de vraag gesteld waarom in Nederland veel evaluaties gescheiden van elkaar geschieden en wat wij van evaluatoren mogen verwachten.<sup>4</sup> De Bruijn (2007) constateert dat de meeste evaluaties uitgaan van een causale benaderingswijze. Er worden fouten geconstateerd die niet gemaakt hadden mogen worden als men zich aan regels en procedures had gehouden. Er wordt een causaal verband gelegd tussen de procedures, de handelingen en de uiteindelijke gevolgen. In plaats daarvan kan ook een contextuele benaderingswijze worden gevolgd. Ook hier worden wel fouten geconstateerd, maar vervolgens wordt op zoek gegaan naar de redenen waarom deze fouten zijn gemaakt. Waarom handelde men zoals men deed? Bij de evaluatie – die feitelijk geen evaluatie was – van de gebeurtenissen na het schietdrama in Alphen aan den Rijn hebben wij getracht deze methodiek systematisch te volgen (Van Duin e.a. 2012). Aan de hand van een aantal dilemma's worden de belangrijkste beslissingen en thema's beschreven. Een andere meer neutrale benaderingswijze is de methodiek van Argyris en Schön (1978) waarin onder andere single en double loop leren als vormen van collectief (organisationeel) leren worden onderscheiden. Brandweer Nederland hanteerde deze methode bijvoorbeeld bij hun zelfevaluatie van de Moerdijk-brand.

Interessant in dit verband is ook het recent verschenen boek *Methodische aspecten van het onderzoek naar ongevallen* waarin vertegenwoordigers van de Onderzoeksraad voor Veiligheid en de TU Delft aspecten van methodologisch goed ongevalsonderzoek aangeven. Verschillende theorieën (van Tripod tot het cascademodel) passeren de revue. Mertens gaat in op het systematisch opleiden van ongevalsonderzoekers. Niet iedereen kan zomaar dergelijk onderzoek doen. Onderzoekers dienen kennis te hebben van de betreffende 'body of knowledge'. Ongevallen vinden altijd plaats in een samenspel van techniek, organisatie en mensen het geen 'vraagt om een goed fundament van kennis over wetenschappelijk verantwoorde benaderingen' (p. 230).

In het eerste deel heb ik geprobeerd een op zich plausible andere kijk op de situatie te geven. Anderen zullen weer met een andere duiding komen. Juist dat maakt dat er een discussie gevoerd zou moeten worden of wij in de toekomst nog wel dergelijke evaluaties wensen waarbij zo stevig geoordeeld wordt. Daarbij kan de vraag worden gesteld of er überhaupt wel geleerd zal worden als er zo stevig geoordeeld wordt. Mogelijk is dan vooral sprake van de symboliek van evalueren (Helsloot, 2007). Typerend in dit verband was bijvoorbeeld dat na het te stevige rapport van de IOOV over het optreden na de Moerdijk-brand de regio Midden en West-Brabant zelf met een gefilmde reconstructie kwam, waaruit een veel positiever beeld over het brandweeroptreden naar voren kwam.

Ook kan de vraag opgeworpen worden of er niet minimale eisen gesteld mogen worden aan de onderzoekers? Wie of wat bepaalt wanneer iets goed of fout is? Als je bij voorbeeld, zoals Mertens stelt (p. 245), aandacht hebt voor de veiligheidscultuur of voor het veiligheidsmanagementsysteem, betekent dit blijkbaar dat jij dat belangrijk vindt. Maar is er ook naar vergelijkbare situaties gekeken en als deze er niet zijn, wat zegt dat dan? Mogen wij verwachten dat organisaties de eerste keer dat ze met een (asbest)probleem worden geconfronteerd, gelijk goed zullen optreden? Eigenlijk niet, want wat je zelden doet doe je zelden goed (Vgl. Van Duin, 2011).

Evaluaties zouden eigenlijk beperkt kunnen blijven tot een omvangrijk feitenrelaas, waarbij de nadruk veel meer zou moeten liggen op het verklaren (waarom handelde men zoals men deed?) en het in kaart brengen van de verschillende dilemma's. Laten de lezers zelf maar tot hun oordeel komen.

### Literatuur

- C. Argyris en D. Schön, *Organizational learning: a theory of action perspective*, Reading, 1978.
- J.A. de Bruijn, *Een gemakkelijke waarheid; waarom we niet leren van onderzoekscommissies*, NSOB, 2007.
- M.J. van Duin, *Veerkrachtige crisisbeheersing: nuchter over het bijzondere* (lectorale rede), 2011.
- M. van Duin e.a., *Lessen in Crisisbeheersing; Dilemma's uit het schietdrama in Alphen aan den Rijn*, Politieacademie: Boom/Lemma, Den Haag, 2012.
- I. Helsloot, *Voorbij de symboliek*, Den Haag, 2007.
- F. Mertens, K. van Schaardenburgh-Verhoeve, S. Sillem (red.), *Methodische aspecten van het onderzoek naar ongevallen*, Delft, 2012.

<sup>4</sup> Voor een uitvoerige behandeling hiervan zie M. van Duin, 'Evalueren en evaluaties na ongevallen, rampen en crises in', in: *Recht, Bestuur en Organisatie van Hulpdiensten*, 2012

# De beoordelaars beoordeeld!

In zijn beschouwing op de werkzaamheden van de commissie 'Onderzoek asbestvondst Kanaleneiland' kijkt Menno van Duin kritisch naar de rapportage van de commissie. Hij oordeelt dat de commissie er slechts in beperkte mate in is geslaagd om de problemen te doorgronden. "Evaluatoren zijn over het algemeen veel te veel gericht op oordelen en soms ook veroordelen, en veel te weinig op het begrijpen". De commissie heeft het oordeel van Menno van Duin serieus bekeken, maar deelt zijn conclusie niet. Begrip hebben voor een besluit of handeling betekent nog niet dat het besluit of de handeling goed is. Om van de gebeurtenissen te kunnen leren is het belangrijk om scherp te analyseren wat

anders had gekund of soms zelfs anders had gemoeten.

De commissie heeft er voor gekozen om de beleving van de 'slachtoffers', de bewoners van de wijk Kanaleneiland, een centrale plek te geven in het onderzoek. Hiermee doet het onderzoek niet alleen recht aan hen die het heft in handen hadden tijdens de crisis, maar ook aan de 'slachtoffers' van de situatie. Door de feiten boven tafel te krijgen en de beleving, zoals de feiten zijn ervaren door de bewoners weer te geven en daar in samenhang over te oordelen, met alle nuances die daar bij horen, heeft het onderzoek het beeld van een betrouwbare overheid helpen herstellen.

De commissie is tevreden over het feit dat zowel het College van B&W, de raad als de bewoners van Kanaleneiland hun waardering hebben uitgesproken over het onderzoek en dat was zeker niet vanzelfsprekend. De werkzaamheden van de commissie hebben hierdoor bij kunnen dragen aan de verzoening tussen de bewoners en de lokale overheid en daarmee tot herstel van vertrouwen. Daarnaast zijn alle aanbevelingen van de commissie overgenomen, ook die met betrekking tot verbetering van de crisisbeheersing. Overigens is het opvallend dat in het artikel de aanbevelingen worden onderschreven terwijl deze rechtstreeks voortkomen uit de conclusies!



Foto: Bert Spiertz

# Leren van de asbestcrisis

drs Marco Meesters,  
senior onderzoeker en adviseur, COT Instituut  
voor Veiligheids- en Crisismanagement

drs Nico Kaptein,  
manager O+Advies, COT



Foto: Bert Spiertz

## Leren van een crisis

Een crisis biedt, zowel voor de betrokken organisaties als voor andere organisaties waar het ook had kunnen gebeuren, een uitgelezen kans om te leren en om in het vervolg dergelijke situaties (nog) beter aan te pakken. Soms is het voldoende om met betrokkenen in een gezamenlijke sessie terug te kijken en de ervaringen te delen, conclusies te trekken en lessen te onderkennen. Wanneer niet helemaal duidelijk is wat er precies is gebeurd, besloten en gedaan kan het nodig zijn een feitenreconstructie op te stellen, op basis van verslagen, rapporten en gesprekken. Op basis hiervan, en aan de hand van een visie of toetsingskader, kunnen bevindingen, inzichten en aanbevelingen worden verwoord. Al deze zaken kunnen door de organisatie zelf worden gedaan, terwijl ook behoefte kan zijn aan een externe, onafhankelijke en professionele partij. Bijvoorbeeld in het kader van interne en externe verantwoording. Evaluatie speelt ook altijd een belangrijke rol in het verwerken en afsluiten van de crisis. Het is voor betrokkenen belangrijk hun verhaal te kunnen doen, de gebeurtenissen te begrijpen en openstaande vragen te beantwoorden.

Woningcorporatie Mitros wilde graag leren van de asbestcrisis en heeft het COT daarom gevraagd om de gebeurtenissen voor, tijdens en na detectie van asbest te reconstrueren en lessen voor de corporatie te formuleren. Het onderzoek richtte zich daarom op het handelen van de corporatie.

## Lessen uit de asbestcrisis

De belangrijkste les is dat in een crisis aandacht nodig is voor impact. Impact in de zin van de consequenties van maatregelen voor vooral bewoners en omwonenden, maar ook voor de betrokken organisaties. En impact in de zin van de uitstraling van maatregelen. In de asbestcrisis zijn diverse maatregelen genomen vanuit operationeel perspectief en vanuit het voorzorgprincipe. De wijk is afgezet, mensen zijn uit huis geplaatst en asbestonderzoekers en brandweermannen zijn in beschermende kleding de wijk ingegaan. Het meewegen van de consequenties van bijvoorbeeld ontruiming voor bewoners (waaronder vluchtelingen of mensen die de Nederlandse taal niet goed beheersen) en het effect van de mannen in witte pakken op de gevaarperceptie, hadden tot andere keuzes kunnen leiden.

De bestuurlijke advisering over gezondheidsrisico's en impact speelt daarin een belangrijke rol. Het ontbreken van goed toepasbare normen voor kortdurende asbestbesmetting in bewoond gebied gecombineerd met het grote gepercipieerde risico van asbest voor de volksgezondheid, bemoeilijkten de bestuurlijke besluitvorming. Het is aan de adviseurs met technische kennis om in dit soort situaties de (acute) gezondheidsrisico's te duiden.

Een andere les is het belang van duidelijkheid in het grijze gebied tussen de corporatie en de crisisorganisatie van de overheid. De onduidelijkheden over taken en verantwoordelijkheden hebben een effectieve aanpak van de crisis bemoeilijkt.

Onder tijdsdruk, in onbekende situaties, met een onbekende gevaarstelling, is het moeilijk om ruimte te nemen voor reflectie en diagnose. Een goede voorbereiding kan daarbij helpen. Voorbereiding mag en moet proportioneel: geen vuistdikke handboeken en protocollen, maar nadenken over risico's en mogelijke crises, processen van alarmering en opschaling en uitgangspunten voor besluitvorming in geval van crisis. Ook het verkennen van de raakvlakken met de lokale crisismanagementstructuren, samen met sleutelpersonen in die structuren, past onze inziens bij een voorbereiding.

De asbestcrisis in Kanaleneiland vertoont qua aard en dynamiek grote gelijkenissen met andere 'gezondheids crises': situaties waarin in de beleving grote risico's bestaan voor de volksgezondheid en die vanwege de complexiteit moeilijk zijn te duiden. Betrokkenen verwachten een antwoord, veilig of niet?, terwijl een dergelijk antwoord niet te geven is. Andere voorbeelden zijn de Sterigenics casus in Zoetermeer en Chemie-Pack in Moerdijk. Bovenstaande lessen zijn dan ook breder toepasbaar.

# Crisisbeheersing naar een substantieel hoger niveau

## Tien verbetervoorstellen

In het Magazine van december 2012 concludeert professor Erwin Muller dat het crisismanagement in Nederland de laatste jaren sterk is verbeterd. De vraag is of deze analyse juist is. Ontegengesteld is er kwantitatief veel veranderd, maar kwalitatief gezien staat het er minder rooskleurig voor. Bij vrijwel elke crisis zie je dezelfde fouten terugkomen. Hoe is dat te verklaren? Met dit artikel geven wij een kritisch tegengeluid en tonen we aan welke structurele problemen er zijn. Met tien verbetervoorstellen kan volgens ons de crisisbeheersing in Nederland naar een substantieel hoger niveau.

### 1. Veiligheidsregio's of provincies?

Om de crisisbeheersing in Nederland te verbeteren zijn er 25 veiligheidsregio's opgericht. Is dit wel een slimme keuze geweest? Een adagium is namelijk dat 'het beheer' het 'gezag' dient te volgen en niet andersom. Het is onjuist de structuur van de hulpdiensten als uitgangspunt te nemen en daar de bestuursstructuur op aan te passen. Nederland is bovendien veel te klein voor 25 veiligheidsregio's. Hetzelfde gevaar ligt op de loer nu de nationale politie is georganiseerd volgens de gerechtelijke landkaart. Binnen afzienbare tijd zal de discussie over tien veiligheidsregio's losbarsten. In de structuurdiscussie is het veel logischer het Thorbecke model te hanteren. Wanneer op deze in ons staatsbestel gewortelde gezagsstructuur het 'beheer' wordt aanpast, dan zou het resultaat zijn: 12 politiekorpsen, 12 brandweerkorpsen, 12 GHOR regio's, 12 waterschappen en 12 arrondissementen. Bij opschaling boven gemeentelijk niveau ligt de verantwoordelijkheid bij de provincie en boven provinciaal niveau bij het Rijk. Het is teleurstellend dat deze discussie onvoldoende wordt gevoerd en dat met de Wet op de Veiligheidsregio's een nieuwe (veiligheid)bestuurslaag is geïntroduceerd die de crisisbesluitvorming onnodig ingewikkeld maakt.

### 2. Focus van fysieke naar integrale veiligheid

Het merendeel van de veiligheidsregio's houdt zich bezig met (klassieke) rampenbestrijding en niet met (moderne) crisisbeheersing. De focus ligt op fysieke veiligheid. Dit staat haaks op de visie die is vastgelegd in de nationale veiligheidsstrategie. Deze schrijft voor dat de veiligheidsregio's zich naast fysieke veiligheid ook moeten richten op territoriale veiligheid, ecologische

veiligheid, economische veiligheid en politieke/sociale veiligheid. Waarom analyseren de veiligheidsregio's bijvoorbeeld niet de gevolgen van de economische (krediet) crisis op regionaal niveau? Hoeveel bedrijven gaan failliet? Wat is de toename van de criminaliteit? Wat is het extra appèl op de geestelijke gezondheidszorg? Enzovoorts. Dit zijn interessante thema's die ook spelers als de directeur van de Kamer van Koophandel en de bancaire sector aan tafel uitnodigen.

### 3. Crisisbeheersing in gemeenten

De gemeente is primair verantwoordelijk voor crisisbeheersing en rampenbestrijding. Bestuurlijk gezien is veiligheid binnen de gemeente versnipperd. Meer en meer ontstaat de roep om een wethouder integrale veiligheid. Deze 'deskundige' zal dan ook in crisis-situaties als voorzitter van het beleidsteam optreden. Daarmee heeft de burgemeester de handen vrij om invulling te geven aan de rol van boegbeeld voor de samenleving. De gemeentesecretaris is ambtelijk de hoogst verantwoordelijke adviseur crisisbeheersing. Hij doet dit er even bij. Dat kan niet. Crisisbeheersing en integrale veiligheid is een vak apart en vergt veel kennis en ervaring. Het verdient aanbeveling een senior deskundige integrale veiligheid dichter tegen de bestuurslaag aan te positioneren, temeer daar de ambtenaren openbare orde en veiligheid veelal diep in de organisatie zijn gepositioneerd. Deze laatste categorie personeel heeft een omvangrijke portefeuille aan taken en zou professioneler moeten worden geschoold in crisisbeheersing en veiligheidsvraagstukken dan nu het geval is.

#### 4. Publiekprivate samenwerking

De publieke sector richt zich voornamelijk op responsmanagement en de private sector op risicomanagement. Beide sectoren werken veelal los van elkaar. In 2007 was er een opleving met de Taskforce Management Overstromingen en het Nationaal Adviescentrum Vitale Infrastructuur, maar snel daarna divergeerden de sectoren weer, een enkel lokaal convenant daargelaten. Het Veiligheidsberaad en VNO-NCW kunnen hier verbetering in aanbrengen door bijvoorbeeld vanuit de belangrijkste vitale sectoren liaisons af te vaardigen binnen de veiligheidsregio's en het LOCC. Daarmee kunnen geïntegreerde planvorming, gezamenlijk opleiden en trainen, kennis- en relatienetwerken worden gerealiseerd. Er valt nog veel van elkaar te leren. Die kansen worden nog onbenut gelaten.

#### 5. Defensie als structurele veiligheidspartner

Defensie is sinds 2005 structureel partner in de veiligheidsregio's. Toch komen vraag en aanbod nog onvoldoende tot elkaar. Hoe valt dit te verklaren? Defensie is binnen de veiligheidsregio's slechts vertegenwoordigd met een officier veiligheidsregio op uitvoerend niveau. De aanwezigheid op tactisch (veiligheidsdirectie) en strategisch (bestuurlijk niveau) niveau ontbreekt. Dit is het niveau waar het beleid wordt vastgesteld. Verder gaat het altijd over de inzet van de middelen van Defensie. Nog onvoldoende rendement wordt gehaald uit 'netcentrische' besluitvorming, leiderschap, Research & Development en het opzetten van oefeningen waarin Defensie is gespeciali-

seerd. Verder is binnen Defensie de bestuurslaag nog onvoldoende doordrongen van de mogelijkheden die Defensie kan benutten in de civiele rampenbestrijding, wordt nog te weinig samengewerkt tussen de vier krijgsmachtdelen en wordt vrijwel geen aandacht besteed aan dit onderwerp in de opleidingen binnen Defensie. Inmiddels is op ministerieel niveau een project Versterking Civiel-Militaire Samenwerking (VCMS) gestart dat tot verbetering moet leiden.

#### 6. Crisismanagement op rijksniveau

Waarom staat de kredietcrisis niet in de Nationale Risicobeoordeling? Waarom is er geen multidisciplinaire en geïntegreerde aanpak van de economische crisis? Waarom zijn de nationale oefeningen zo voorspelbaar in de uitkomsten? Om deze knelpunten op te lossen moet er een GRIP 5 worden geïntroduceerd. Naar analogie van de opschalingsprocedure op lokaal en regionaal niveau moet ook de ministeriële commissie Crisisbeheersing (MCCb) binnen één uur operationeel kunnen zijn, waarbij vanuit het LOCC en het NCC de operationele informatie wordt ingebracht. Een ander verbeterpunt is de erkenning van het Ministerie van Veiligheid en Justitie als coördinerend departement met doorzettingsmacht bij nationale rampen en crisisbeheersing. Crisismanagement is namelijk voor generalisten en niet voor specialisten. Ten slotte zal er een andere kijk op en invulling van grootschalige oefeningen moeten komen. Hier kan de publieke sector nog veel leren van bijvoorbeeld de luchtvaartsector waar men veel realistischer oefent.

#### 7. Bewustwording bij bestuurders en toezicht-houders

Het blijkt dat de bewustwording en kennis van crisismanagement bij bestuurders en toezichthouders veelal tekortschiet. Deze trend zie je binnen de zorgsector, de onderwijssector en binnen het openbaar bestuur. Hoe kan dat? Eenvoudigweg door de complexiteit van het veiligheidsdomein. Daardoor krijgen bestuurders veel adviezen vanuit de verschillende ambtelijke disciplines en is het moeilijk te selecteren en te prioriteren. Dit moet structureel verbeteren. Recent heeft het COT





Instituut voor Veiligheids- en Crisismanagement bestuurders geadviseerd: creëer een bestuurlijk dashboard veiligheid; wees realistisch, transparant en eerlijk over veiligheid en ontwikkel een visie op veiligheid. Naast de adviezen van het COT is het raadzaam een veiligheidsdeskundige dicht tegen het bestuur te positioneren, die verantwoordelijk is voor een integraal stafadvies over deze materie.

#### **8. Crisis- en risicocommunicatie als bestuurlijke tool of management**

Bij rampen en crisissituaties gaat het vrijwel altijd fout in de crisiscommunicatie. Bestuurders die met reputatiecommunicatie bezig zijn en nog onvoldoende gewend zijn aan de snelheid en dynamiek van de internetsamenleving zijn hiervan een sprekend voorbeeld. Het wordt tijd communicatie als tool of management bovenaan de bestuurlijke agenda te plaatsen en niet als sluitpost. De crisiscommunicatie moet op professionele leest worden geschoeid. De focus moet liggen op relatiecommunicatie waarbij het belang van de getroffen centraal staat. Communicatiedeskundigen Hans Siepel en Frank Regtvoort stellen dat het bij crisiscommunicatie gaat over drie basisprincipes: informatieverstrekking, schadebeperking en betekenisgeving. Daarnaast zal de lokale bestuurder de risicocommunicatie dicht bij de bevolking moeten brengen. Dat zal de burger meer aanspreken dan de Rijksoverheidspotjes, waarvan is aangetoond dat ze geen rendement hebben.

#### **9. De zorg- en onderwijssector**

De zorgsector is zich sinds 2008 beter aan het voorbereiden op grootschalige rampen en crisissituaties. Er worden integrale crisisplannen gemaakt, risicoanalyses worden afgestemd op die van de veiligheidsregio's en er wordt veel aandacht besteed aan opleidingen, trainingen en oefeningen. De resultaten zijn inmiddels zichtbaar en dat alles is mede mogelijk gemaakt door een subsidie (OTO stimuleringsprogramma) van de

minister van VWS. De onderwijssector is nog niet zover. Vaak gaat het hier mis zoals we regelmatig in het buitenland zien, maar ook de gebeurtenissen in Hoogerheide en Zoetermeer staan nog vers op ons netvlies. Directies van scholen en universiteiten zouden veel meer kunnen doen aan risicobeheersing en crisismanagement. Waarom niet op korte termijn een versterkingsprogramma starten met steun vanuit het ministerie van Onderwijs, Cultuur en Wetenschap? Het zou triest zijn wanneer een dergelijk programma pas start na een grootschalig schietincident op een Nederlandse school.

#### **10. Leren van rampen uit het verleden**

Een standaard reactie na een ramp is een of meerdere onderzoeken door de Inspectie Veiligheid en Justitie, Inspectie voor de Gezondheidszorg of de Onderzoeksraad voor Veiligheid. In deze doorgaans dikke rapporten staat de schuldvraag centraal en is moeilijk traceerbaar welke structurele verbeteroplossingen kunnen worden gerealiseerd. Bovendien wijst de praktijk uit dat men deze rapporten moeilijk kan communiceren met de veiligheidsregio's, gemeenten en bevolking en dat de inhoud snel wordt vergeten. Het is van belang dat er veel meer lessen uit rampen en crisissituaties worden geborgd op regionaal niveau. Een sectie lessons learned in de veiligheidsregio kan daartoe een prima oplossing bieden. Door goede analyses van nationale en internationale rampsituaties kunnen snel en adequaat verbetermaatregelen worden geïmplementeerd. Ook bij crises in andere regio's kunnen deze secties initiëren dat elders opgedane expertise snel beschikbaar wordt gesteld.

#### **Nawoord**

Crisisbeheersing moet eenvoudig worden georganiseerd. Uit het bovenstaande blijkt dat de organisatie van de crisisbeheersing nogal complex is. Terug naar het Thorbecke model is ons voorstel. Daarnaast is het van belang dat de veiligheidsregio's anno 2013 hun focus meer richten op de moderne crisisbeheersing. Het gewenste resultaat wordt ook eerder bereikt door een betere publiekprivate samenwerking, meer awareness bij bestuurders en het op professionele wijze betrekken van defensie als volwaardig veiligheidspartner. Het kennis- en bewustwordingsniveau van crisisbeheersing binnen de gemeenten, veiligheidsregio's, zorg- en onderwijssector zal aanzienlijk moeten worden verbeterd en we dienen beter te leren van rampen uit het verleden. Ook crisismanagement op rijksniveau alsmede de risico- en crisiscommunicatie dienen fundamenteel te worden verbeterd en als aandachtsveld prominent op de bestuurlijke agenda te worden geplaatst. De tijd is nu rijp voor een structurele verbeteringslag. Alle hoop is gevestigd op de recent door minister Opstelten ingestelde Evaluatiecommissie Hoekstra.



Burgemeester Gerritsen gemeente De Bilt:

# “Communicatie moet bestuurders coachen bij crises”

Burgemeester Arjen Gerritsen van de gemeente De Bilt is sinds 1998 bestuurlijk actief. Eerst als wethouder in gemeente Wierden en daarna als jongste burgemeester van Nederland in Haren. Sinds 2007 is hij burgemeester van gemeente De Bilt. Tijdens zijn loopbaan heeft hij een zwak gekregen voor de hulpverleningspoot. Vanuit de opstart-fase van de Hulpverleningsdienst Groningen heeft hij meegekregen dat ‘elkaar helpen altijd handig is’. Nu is hij lid van de Bestuurscommissie Risico- en Crisiscommunicatie en Bevolkingszorg van Veiligheidsregio Utrecht.

## Crisis: overheid én burgers moeten leiderschap tonen

“Wat mij aanspreekt in het vakgebied van crisisbeheersing is dat ‘je het ook echt mag doen’ als burgemeester. De hectiek van een crisis daagt me uit, is zelfs mooi. Daarbij komt dat een gemeente bij een crisis en bij risico- en crisiscommunicatie vrij principieel toch vooraan staat. Volgens de wet ligt het opperbevel bij crisis nou eenmaal bij de burgemeester. Een GRIP 3 wil zoveel zeggen als ‘burgemeester, je moet aan de bak’. Die éénhoofdige lijn spreekt mij wel aan”, aldus Gerritsen.

## Leiderschap is een mindset

“Een keuze voor het burgemeesterschap impliceert dat je je verantwoordelijk voelt voor mensen en processen en daar leiding aan wilt geven. Niet alleen politiek of bestuurlijk, maar juist zelfs bij een ramp of crisis. Als burgemeester moet je dit eigenlijk van nature hebben. Maar het geldt ook voor andere overheidsfuncties en voor burgers. Het is een vorm van mindset. Je moet eigen leiderschap durven tonen. De overheid die van de wieg tot het graf voor je zorgt, is niet meer van deze tijd. Dit is niet erg. Het is erg dat er grote groepen zijn die denken dat dit nog wel zo is.”

## Verantwoordelijkheid van de media

“Er moet ruimte zijn om te kunnen vertellen dat de overheid bepaalde dingen niet kan leveren. In onze samenleving horen risico's er nu eenmaal bij. Een risicoloze samenleving willen en daar de overheid op aanspreken, irriteert me omdat het een vorm van weglopen voor eigen verantwoordelijkheid is. Ook de media doen daar aan mee. Het wantrouwen, de argwaan van de media bij het handelen van de overheid bij crises vind ik op z'n zachtst gezegd apart. Natuurlijk moeten media de overheid scherp volgen, maar media hebben ook een verantwoordelijkheid voor het kanaliseren van de publieke opinie. Dat is wat anders dan ‘spinnen’. Goede journalistiek is zich bewust van die rol.”

## Communicatiedeskundigen moeten bestuurders coachen

“Bij de benadering van risicocommunicatie moet worden onderkend, dat je daar zelf verantwoordelijk voor bent. Bestuurders moeten op die verantwoordelijkheid worden gecoached. Daar lijkt mij een communicatie-unit leiding in te moeten zijn. Ik verwacht van mijn communicatieclub dat zij letten op de maatschappelijke onderstroom; zeker tijdens crises. En ze

moeten mij, de bestuurder, daarop wijzen en met mij beoordelen of en hoe ik of iemand anders daarop moet reageren. We hebben tijdens crisis allemaal een rol te vervullen en dus ook op voorhand al. Vertel elkaar wat je doet en kunt en wat je niet doet en niet kunt.”

## Strategische communicatie in het beleidsteam

“Ik denk zelf erg na over waar ik mijn rol als burgemeester in crisisverband het beste kan vervullen. De huidige structuur van de crisisorganisatie betreft de burgemeester veel te veel bij de operatie. Je loopt het risico dat je gaat ‘meeblussen’. Je vermorst tijd en gelegenheid om je te richten op wat er door het incident in de samenleving gebeurt. Juist daar ligt je rol. Eigenlijk moet je een groep strategische communicatieadviseurs om je heen hebben in een beleidsteam. Ik pleit dus voor een heel andere focus, gericht op maatschappelijke effecten van het incident; niet op hoe hoog de vlammen uit het dak schieten of waar de afzettingen staan. Van buitenaf wordt je hier trouwens goed bij geholpen. Het Nederlands Genootschap van Burgemeesters is een mooie vertrouwenwekkende club die burgemeesters uitstekend terzijde staat met juist die gerichtheid.”

# Slachtoffer Informatie Systematiek (SIS)

Uit evaluaties van Nederlandse crisissituaties en rampen van de afgelopen tien jaar komt naar voren dat de snelheid waarmee verwanten van slachtoffers geïnformeerd worden, moet verbeteren. Voor verwanten van slachtoffers telt elke minuut, elk uur. Vanuit dit besef streven alle professionele hulpverleners er naar sneller informatie over familieleden te geven die (mogelijk) betrokken zijn bij een crisis. Het Veiligheidsberaad heeft op 23 november 2012 het besluit genomen om een landelijke voorziening te regelen voor slachtofferregistratie en verwanteninformatie.

Directe aanleiding voor de start van het project SIS in 2010 was de politieke discussie over de organisatie en uitvoering van het informeren van verwanten van slachtoffers bij grootschalige incidenten. De vuurwerkramp in Enschede en de cafébrand in Volendam hadden eerder laten zien dat verwanteninformatie een lastig proces is waar de overheid veel moeite mee had. Twee grote incidenten in 2009, de Poldercrash en de aanslag tijdens de Koninginnedagviering in Apeldoorn lieten eenzelfde beeld zien. Belangrijke knelpunten waren het bijeenbrengen van informatie van verschillende instanties en de snelheid waarmee verwanten geïnformeerd konden worden. De ontevredenheid met de huidige systematiek van verwanteninformatie was begin 2010 aanleiding voor een debat in de Tweede Kamer.



Foto: Arthur Wijnen

SIS is een gezamenlijk project van de gemeenten, GHOR en Politie. Onder de noemer SIS hebben deze partijen afspraken gemaakt over de uitwisseling van slachtofferinformatie en de daarbij horende taakverdeling en communicatieprocessen tijdens en na een ramp op nationale bodem. Nu duidelijk is hoe de systematiek wordt geïmplementeerd, volgt de fase waarin de organisatie van SIS vorm krijgt.

## Kanteling in denken

Het primaire doel van slachtofferregistratie was en blijft het informeren van verwanten. Alexander Meijer, voorzitter stuurgroep SIS: "Het uitgangspunt is het sneller kunnen informeren van verwanten van niet-zelfredzame slachtoffers. De hulpverlening aan zwaargewonden heeft in de acute fase van een ramp prioriteit. De slachtoffers die licht- of niet gewond zijn laten tegenwoordig zelf vaak weten dat zij het goed maken, zij lopen weg van de rampplek en bellen hun familie met hun mobiele telefoon. De overheid kan de zelfredzame slachtoffers faciliteren (bijvoorbeeld door het aanbieden van een telefoon), maar hoeft het informeren van verwanten van deze slachtoffers niet voor ze te regelen."

## Focus hulpverlening op niet-zelfredzame slachtoffers

Dit is anders als het gaat om dodelijke of zwaargewonde slachtoffers. SIS heeft als uitgangspunt dat de overheid vooral hier haar verantwoordelijkheid neemt. De inspanning van de overheid moet zich tijdens de acute fase richten op het bijeenbrengen van informatie en het informeren van verwanten van deze slachtoffers. De overheid moet zich in de acute fase niet richten op het registreren van alle slachtoffers. De focus op niet-zelfredzame slachtoffers leidt ertoe dat verwanten van dodelijke en zwaargewonde slachtoffers sneller geïnformeerd kunnen worden. Deze kanteling in denken is ook overgenomen in het rapport Bevolkingszorg op orde: de vrijblijvendheid voorbij.

## SIS sluit aan op dagelijkse werkzaamheden hulpverleners

Mensen houden in crisissituaties vast aan hun dagelijkse routine, daarom is het belangrijk SIS aan te laten sluiten bij die dagelijkse routine van professionals. Het bijeenbrengen van informatie, het identificeren van een dodelijk of zwaargewond slachtoffer en het informeren van familie over het slachtoffer vraagt specifieke expertise. Deze expertise is in verschillende kolommen



terug te vinden. De getroffen gemeente blijft verantwoordelijk voor het proces slachtofferregistratie, maar zal voor de uitvoering handiger gebruik maken van de andere kolommen en andere organisaties.

### Landelijke oplossing is keuze voor opbouw kennis en expertise

Het Veiligheidsberaad heeft in november 2012 gekozen voor een landelijke uitwerking van de systematiek, waarbij er één front- en één backoffice komt voor heel Nederland. Het argument van opbouwen en behouden van kennis en ervaring bij het informeren van verwanten is daarbij doorslaggevend geweest, naast de verwachte financiële voordelen van de landelijke organisatie. De keuze van het Veiligheidsberaad houdt in dat er één centraal telefoonnummer en website komen voor het verzamelen van informatie over mensen die mogelijk betrokken zijn bij een ramp.

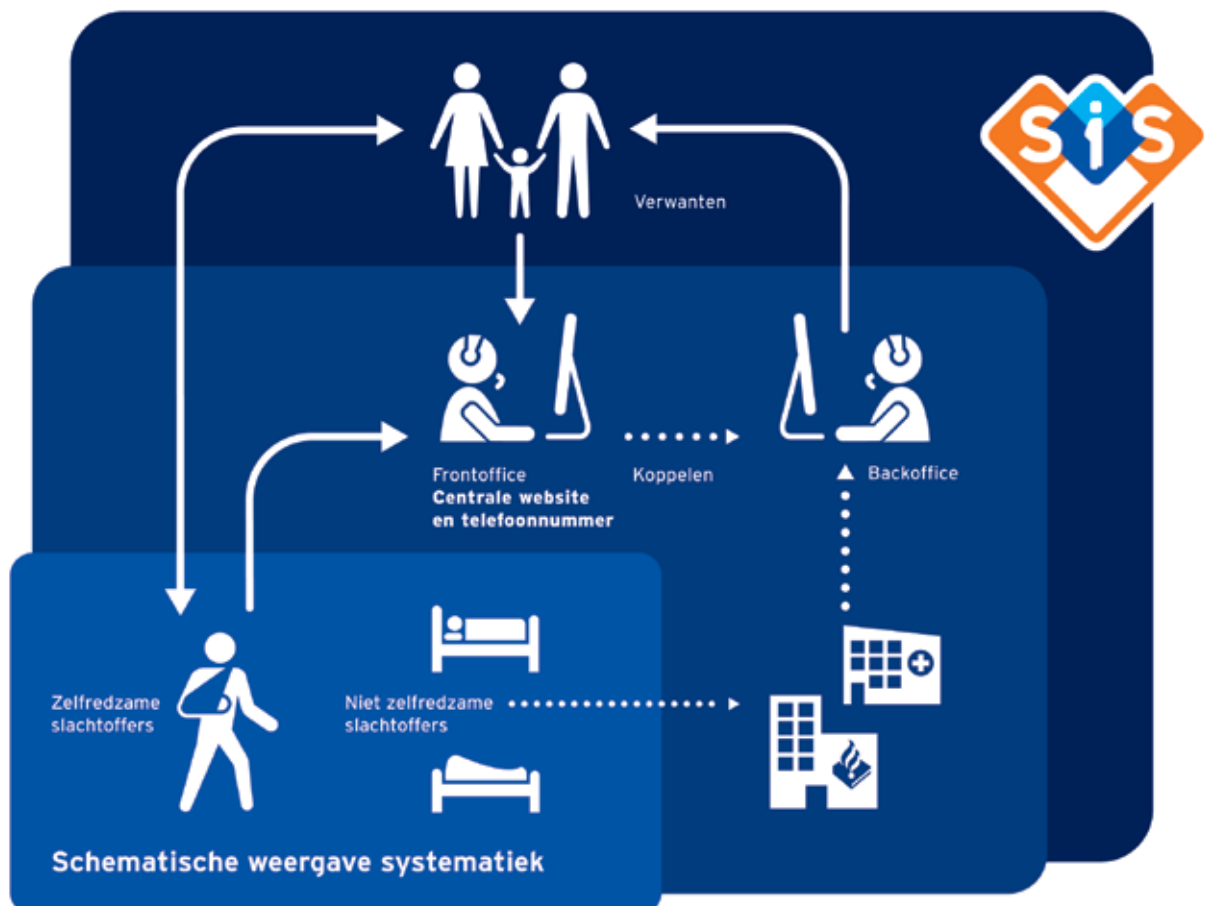
### Hoe werkt SIS?

Medewerkers achter het centrale telefoonnummer (de frontoffice) zijn getraind in het telefonisch helpen en informeren van verwanten. De frontoffice medewerkers verzamelen belangrijke informatie en geven deze gegevens via het registratiesysteem door aan de backoffice, waar de gegevens van verschillende bronnen

(frontoffice, ziekenhuizen, mortuaria, politie, gemeenten et cetera) bijeenkomen. De backoffice valideert, vult gegevens aan en matcht deze, zodat de slachtoffers van de ramp gekoppeld kunnen worden aan de mensen die vermist worden en hun verwanten geïnformeerd kunnen worden. De front- en backoffice worden aangestuurd door een chef die op gezag van en met verantwoording aan de algemeen commandant bevolkingszorg van de gemeente opereert. De burgemeester wordt geregeld geïnformeerd over de stand van zaken voor het duiden van de ramp. Tot slot worden de gegevens van de slachtoffers gebruikt voor het bieden van nazorg.

### Handreiking met ziekenhuizen

Een ander belangrijk knelpunt is de uitwisseling van gegevens tussen openbaar bestuur en ziekenhuizen. Landelijke vertegenwoordigers van het openbaar bestuur en de ziekenhuizen hebben in december 2012 de 'Handreiking afspraken tussen openbaar bestuur en ziekenhuizen over slachtofferinformatie bij rampen en crises' opgesteld om deze informatie-uitwisseling te verbeteren. Michiel Hoorweg, secretaris projectgroep SIS: "In het verleden was er vaak onduidelijkheid over de mogelijkheid om slachtoffergegevens uit te wisselen tussen ziekenhuizen en het openbaar bestuur, onder



## Stroomschema slachtofferinformatie

### Legenda

zkh

DPG

backoffice slachtofferinformatie

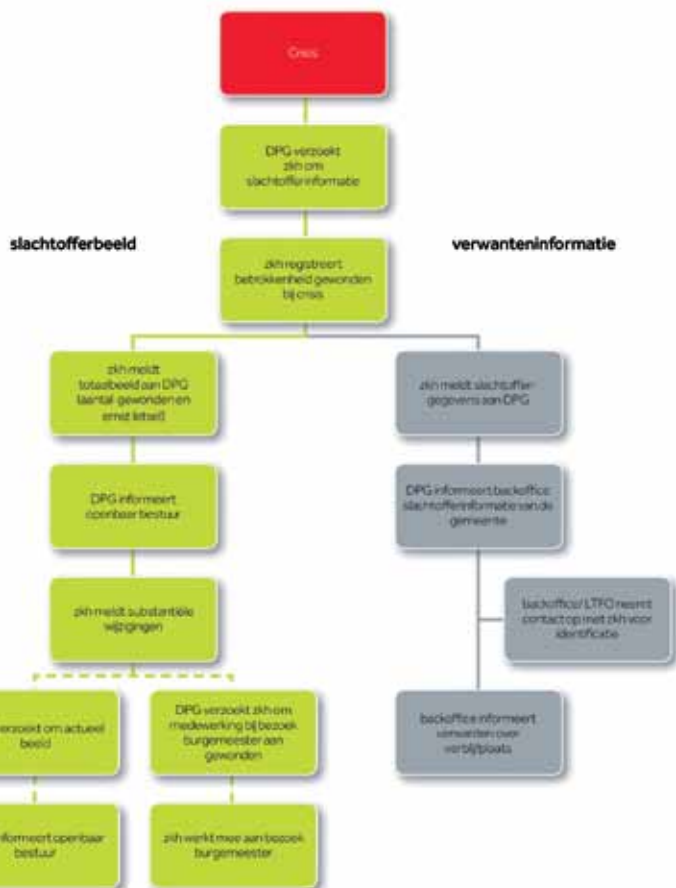
LTFO

ziekenhuis

directeur publieke gezondheid

team van de gemeente dat zorgt voor identificatie van slachtoffers en informatie aan (mogelijke) verwanten

Landelijk Team Forensische Opsporing van de politie



### Geen eigen gemeentelijk systeem slachtofferregistratie

Door de landelijke implementatie van SIS hoeven niet alle gemeenten zelf een voorziening te hebben voor slachtofferregistratie bij crises. Vanaf 2014 kunnen gemeenten de landelijke front- en backoffice inzetten om de informatie bijeen te brengen en verwanten te informeren. Uiteraard is het resultaat van de slachtofferregistratie ook voor de nafase van belang. De gegevens van SIS zullen dan ook voor de nafase beschikbaar worden gesteld. Aan de zelfredzame slachtoffers wordt tijdens de nafase verzocht om zichzelf te melden bij de gemeente of andere hulpverleningsinstanties als zij gebruik willen maken van bepaalde faciliteiten van de nazorg of omwille van schaderegistratie. Dit sluit aan bij de reguliere werkwijze van een gemeente. De gemeente communiceert immers waarvoor een burger bij haar kan aankloppen. Het is aan de burger of zij van de dienstverlening gebruik wil maken. Ook kunnen betrokkenen via die route meewerken aan het opsporingsonderzoek van de politie.

### Realistischer boodschap aan burgers

Alexander Meijer: "De overheid kan de zelfredzaamheid van burgers voorafgaand aan een ramp vergroten door realistischer te communiceren over de rol van een overheid bij een crisis. In risicocommunicatie kunnen overheden en hulpverleningsorganisaties duidelijker naar voren laten komen dat een hulpverlener zich in eerste instantie zal richten op dodelijke en zwaargewonde slachtoffers. Zelfredzamen hebben een eigen verantwoordelijkheid in het informeren van hun naaste omgeving. Namens de projectgroep wil ik de Ministeries van VenJ en VWS bedanken voor hun steun, dat geldt ook voor het draagvlak dat wij kregen bij de betrokken kolommen en de ketenpartners. Dankzij de goede samenwerking kunnen we nu echt beginnen met de implementatie van SIS."

andere vanwege het medisch beroepsgeheim. In de handreiking is nu met de landelijke koepels uitgewerkt in welke situaties en onder welke voorwaarden het wel kan. Aan de hand van deze handreiking kan de GHOR haar rol in de slachtoffer informatie systematiek naar verwachting goed waarmaken."

Het ziekenhuis en het openbaar bestuur spreken conform de handreiking af dat de directeur publieke gezondheid bij een crisis zo snel mogelijk een melding maakt aan de betrokken ziekenhuizen en hen verzoekt om slachtofferinformatie. Het ziekenhuis zorgt dan voor een herkenbare registratie van de slachtoffers en stuurt zo spoedig mogelijk een slachtofferbeeld en eventueel (individuele) slachtoffergegevens aan de directeur publieke gezondheid. Deze zorgt vervolgens voor de informatievoorziening aan het openbaar bestuur en andere hulpverleners.

### Vervolg

Door het besluit van het Veiligheidsberaad is een belangrijke stap genomen in het verbeteren van het proces slachtofferregistratie en verwanteninformatie. Dit jaar gaat het project verder. De front- en backoffice zullen in opdracht van het Veiligheidsberaad worden ingericht en de aansluiting met de Veiligheidsregio 's zal verder worden uitgewerkt. Het streven is om begin 2014 volgens deze nieuwe werkwijze te gaan werken.

### Meer informatie of SIS volgen?

De handreiking voor afspraken met ziekenhuizen is onder andere te vinden op [www.ghor.nl](http://www.ghor.nl). Meer informatie over de uitgangspunten, de systematiek en het vervolgtraject zijn terug te vinden op [www.projectsvs.nl](http://www.projectsvs.nl). Twitter: @projectsis, linked-in: SIS Sneller informatie voor verwanten bij crisissituaties NL



# Aandacht voor risico's digitaal verkeer door campagne Alert Online

Online is steeds meer de norm. Het aantal uren dat men off line is, neemt snel en zienderogen af. Treinreizigers zijn vergroeid met hun smartphone en televisiekijken doe je tegenwoordig met een tweede scherm op schoot. Geen overbodige luxe dus om meer aandacht te vragen voor de risico's die het hedendaagse digitale bestaan met zich meebrengt en meer bewustwording te creëren bij de online Nederlander. Dat was dan ook precies het doel van de campagne Alert Online die de NCTV samen met anderen van 12 tot 22 november heeft gevoerd.

Niet toevallig vond de start van de campagne plaats in het Utrechtse hoofdkwartier van de Rabobank. Want het bankwezen is natuurlijk direct gebaat bij klanten die zich tijdens het internetbankieren alert gedragen. Maar de locatie stond vooral symbool voor de samenwerking tussen overheid en bedrijfsleven op het terrein van cyber security. "Op het gebied van cyber security geldt: samenwerking werkt!", benadrukte minister Opstelten van Veiligheid en Justitie bij de aftrap van de campagne Alert Online. De publiekprivate samenwerking in het digitale veiligheidsdomein beperkt zich niet tot de invulling van beleid en regelgeving, maar is ook de basis van het voorkomen en beperken van incidenten en het vergroten van de bewustwording. Van dat laatste was Alert Online, waaraan tal van partijen een steentje hebben bijgedragen, een aansprekend voorbeeld.

Al bij het opstellen van de Nationale Cyber Security Strategie in 2010 ging veel aandacht uit naar bewustwording. "Een belangrijke

actielijn in die strategie is versterking van de weerbaarheid tegen ICT-verstoringen en cyberaanvallen", bracht Opstelten in herinnering, "maar effectief maatregelen nemen om je weerbaarheid te vergroten kun je pas, als je weet wat nu eigenlijk de risico's zijn." Dat het met de kennis van de risico's die iedereen tijdens het online communiceren loopt, niet al te best is gesteld, blijkt uit recent onderzoek dat kort voor de start van de campagne in opdracht van de NCTV is uitgevoerd. Er is nog flink wat werk aan de winkel, concludeerde de minister, waarna hij de daad bij het woord voegde en het startsein voor de campagne gaf.

## Spotjes

De helft van de burgers heeft überhaupt geen idee wat cyber security nu eigenlijk is, zo toonde het onderzoek aan. Een overgrote meerderheid gebruikt wachtwoorden die niet voldoen aan de veiligheidsvoorschriften en de risico's van cybercriminaliteit worden danig onderschat. Specifiek onderzoek naar de mate van bewustzijn onder bedrijven en overheden geeft een

vergelijkbaar beeld: er is nog veel te verbeteren. Zo voeren de meeste bedrijven geen digitaal veiligheidsbeleid en weten de werknemers dus niet hoe ze zich achter de computer horen te gedragen. De rijksoverheid heeft wel de nodige spelregels vastgelegd, maar daar ontbreekt het vaak aan handhaving. Tijdens de tiendaagse campagne zal het weinigen zijn ontgaan dat meer alertheid in het digitale verkeer geboden is. Via online banners, radiospots en de website [alertonline.nl](http://alertonline.nl) werd het belang van je bewust zijn van digitale risico's benadrukt. Aan aandacht in de media heeft het in ieder geval niet ontbroken. Later dit jaar wordt het onderzoek onder burgers, bedrijven en overheden herhaald en dat zal duidelijk maken of de alertheid is toegenomen. Aandacht voor veilig gebruik van internet mag niet verslappen; daarom zal ook in 2013 weer een campagne Alert Online plaatsvinden, met nog meer deelnemende organisaties en activiteiten om zo samen de digitale veiligheid van Nederland te verhogen.

De campagnewebsite [www.alertonline.nl](http://www.alertonline.nl) geleidt inmiddels door naar de NCTV: [www.nctv.nl](http://www.nctv.nl). Daar vindt u tips, factsheets en adviezen over cyber security. Ook is er een instructieve film te zien die de veelzeggende titel 'Je bent zichtbaarder dan je denkt' heeft meegekregen. Om te kijken hoe het met uw bewustzijn staat kan een e-learning worden gevolgd.

# Rechtvaardige selectie van patiënten bij een pandemie

In 2009 deed zich een griep-pandemie voor, die bekend werd als 'de Mexicaanse griep'. Het dreigde een griep-pandemie te worden met grote gevolgen. De kans op schaarste op de intensive care was reëel. Het confronteerde intensivisten met mogelijke complexe afwegingen over selectie van patiënten vanwege schaarste op de intensive care. Gelukkig viel het mee, selectie heeft niet plaatsgevonden. Een volgende keer kan het anders gaan. Daarom bracht het Centrum voor Ethiek en Gezondheid (CEG) onlangs een signalement uit over het opstellen van een rechtvaardig selectiebeleid bij een (griep)pandemie. Sturend daarbij was de vraag: "If we are to adequately prepare for a pandemic of influenza, how should we prepare to be ethical?" (Thomas, 2007).



## Schaarste en selectie

Het signalement is geen advies met concrete aanbevelingen, maar bespreekt vooral de ethische overwegingen die aan de orde zijn bij selectie van patiënten op de intensive care als er schaarste is ontstaan door een (griep)pandemie. Er is sprake van een situatie van schaarste wanneer de vraag het aanbod overstijgt. Niet alle patiënten die daarvoor in aanmerking komen kunnen worden opgenomen en behandeld. Er moet een keuze plaatsvinden tussen patiënten op basis van bepaalde criteria, ook wel 'selectie' of 'triage' genoemd. Als patiënten op de intensive care niet de noodzakelijke zorg krijgen, kan dat in veel gevallen leiden tot de dood. Beslissingen zijn daarom schrijnend. Aangezien er zoveel op het spel staat is het van belang dat vooraf rechtvaardige protocollen worden ontwikkeld. Bij selectie van patiënten is rechtvaardigheid in twee opzichten een leidend principe. Bij 'verdelende rechtvaardigheid' gaat het om een rechtvaardige verdeling van schaarse middelen. 'Procedurele rechtvaardigheid' stelt dat voor het opstellen van

inhoudelijk rechtvaardige protocollen, een eerlijk beslissingsproces nodig is.

## Verdelende rechtvaardigheid

Om niet te vervallen in willekeur moet selectie plaatsvinden op basis van relevante verschillen. Maar wat zijn relevante verschillen in medisch en maatschappelijk opzicht? Het concept 'formele rechtvaardigheid' (afkomstig van Aristoteles) is hierbij behulpzaam. Het betekent dat individuen en groepen als gelijken moeten worden behandeld in zoverre zij elkaars gelijken zijn. Het impliceert ook dat ongelijken ongelijk behandeld dienen te worden. Alleen een moreel relevant verschil rechtvaardigt en vereist een verschillende behandeling. Daarbij is het belangrijk steeds zich te realiseren dat "every patient selecting decision is a tragedy, for someone is always consigned to death" (Kilner, 1990). Het CEG-signalement bespreekt ethische overwegingen bij verschillende selectiecriteria. Het signalement biedt geen doorslaggevende oplossing maar het kan helpen bij de keuze voor selectiecriteria. Het overzicht van relevante argumenten voor rechtvaardige selectie en besluitvorming is bedoeld als een handreiking voor het voeren van deze noodzakelijke discussie.

## Procedurele rechtvaardigheid

Vooralsnog ontbreekt publieke of professionele consensus over wat in een crisissituatie rechtvaardig is. Toch zullen er beslissingen genomen moeten worden over het selectiebeleid. Omdat het niet zonder meer duidelijk is wat een rechtvaardige verdeling van schaarse middelen is, wordt het des te belangrijker dat de procedure voor het opstellen van beleid rechtvaardig is.

In een analyse van 45 Amerikaanse nationale griep-pandemie plannen die beschikbaar zijn op internet was de opvallendste bevinding, dat het volledig ontbrak aan een ethische terminologie. In sommige protocollen

werd een 'behoefte aan ethische besluitvorming' genoemd, maar in bijna geen enkel plan komt naar voren hoe ethische besluitvorming moet plaatsvinden (Thomas, 2007). Een opmerkelijke constatering, omdat dit soort beslissingen in de praktijk met veel morele pijn gepaard gaan.

### Anticipatie

Voor protocollen is empirisch bewijs nodig, maar bewijs is niet altijd voorhanden. En zelfs met het beste bewijs zijn de protocollen inherent ethisch van aard. Beslissingen moeten rechtvaardig zijn. Tijdens een crisis is er geen tijd voor deliberatie en weloverwogen keuzen. Toch moeten er lastige keuzen worden gemaakt met schrijnende gevolgen. Is er geen protocol en moeten er tijdens een crisis ad hoc beslissingen genomen worden, dan zet dat de deur wijd open voor persoonlijke willekeur. Daarom is het van groot belang om een protocol klaar te hebben liggen waarin ethische afwegingen voor rechtvaardige selectie van patiënten expliciet worden genoemd.

### Transparantie

Het betrekken van het publiek bij de protocollering is essentieel om vertrouwen te wekken en hun bereidheid te krijgen om mee te werken. Bovendien hebben plannen die zijn gebaseerd op gedeelde waarden en een eerlijk proces de meeste kans van slagen tijdens een pandemie. Als beslissingen en rechtvaardigingen niet transparant en openbaar zijn geeft dat aanleiding tot twijfel of wantrouwen over de vraag of het selectieproces wel op een rechtvaardige manier heeft plaatsgevonden. Er is dan sprake van een gebrekkige democratische legitimiteit.

### Verantwoordelijke partijen

Er zijn drie partijen te onderscheiden, ieder met hun eigen pakket aan verantwoordelijkheden om een crisis en daaruit voortkomend leed zo goed mogelijk te kunnen beperken: de besluitvormers, de uitvoerders en het publiek (burgers). Besluitvormers zijn verantwoordelijk voor het aankondigen voor de crisissituatie. Beslissingen moeten plaatsvinden op het hoogste niveau om de beslissingen autoriteit mee te geven, waardoor uitvoerders hun werk kunnen doen. De uitvoerders zijn verantwoordelijk om de uitvoering van protocollen zo rechtvaardig mogelijk te laten verlopen. Soms zal het gaan wringen, bijvoorbeeld als zij de protocollen niet rechtvaardig achten. Voor die gevoelens moet expliciet aandacht zijn, bijvoorbeeld in de vorm van 'coaching on the spot', om uitvoerders gemotiveerd te houden. Het publiek zal actief betrokken moeten worden bij de discussie over wat rechtvaardige selectie van patiënten is bij een pandemie. Dit is nodig om een breed maatschappelijk draagvlak te creëren en kan later wantrouwen, verzet en chaos



voorkomen. Want juist het publiek zal moeten leven met pijnlijke selectiebeslissingen en zal zich bijvoorbeeld moeten houden aan hygiënevoorschriften om verspreiding tegen te gaan, en kan zich mogelijk inzetten als vrijwilliger.

### Debat tijdig starten

Als zich deze winter een griep pandemie voordoet, zijn we dan goed voorbereid? En wat te doen als absolute schaarste aan bedden ontstaat op de intensive care afdelingen? In die situatie zullen niet alle patiënten de noodzakelijke zorg kunnen krijgen wat in het ergste geval hun overlijden tot gevolg heeft. Deze schaarste plaatst professionals en beleidsmakers daarom voor lastige ethische afwegingen. Want welke patiënten gaan dan voor? Patiënten die al opgenomen waren of die nieuw binnenkomen? Patiënten die er het slechtste aan toe zijn of juist patiënten met de beste kansen? Krijgen jongeren voorrang? Zorgverleners zelf? En wie beslist daarover? Omdat een eenduidig antwoord op deze vragen niet mogelijk is, is het van belang tijdig een discussie te voeren over wat rechtvaardige selectiecriteria zijn en wat een rechtvaardige besluitvormingsprocedure is bij een pandemie, vindt het CEG. Het CEG zet zelf de eerste stap en opende op 11 februari in het AMC het debat door in discussie te gaan met intensivisten, bestuurders beleidsmakers en ethici.

Een exemplaar van het signalement is aan te vragen via [info@ceg.nl](mailto:info@ceg.nl) of te downloaden via de website [www.ceg.nl](http://www.ceg.nl).

### Literatuur

- J.C. Thomas, N. Dasgupta, A. Martinot, 'Ethics in a Pandemic: A Survey of the State Pandemic Influenza Plans', in: *American Journal of Public Health* 2007; 97 (1), 26-31.
- J.F. Kilner, *Who lives? Who dies? Ethical criteria in patient selection*, New Haven & London: Yale University Press, 1990.

Opleidingskaders en functieprofielen GROOTER zorgen voor professionalisering

# Oranje kolom uit de startblokken

'De oranje kolom als spin in het web. Dat maakt het verschil als crisis ontstaat.' Een populaire vertaling van de doelstelling van project GROOTER, winnaar van de Don Berghuijs Award 2012. Hoe je het ook verwoordt: er ligt op het vlak van crisisbeheersing een forse uitdaging voor de gemeentelijke kolom om te professionaliseren. De projecten GROOT en vervolgens GROOTER dragen hieraan bij door, samen met professionals uit het hele land en de Universiteit van Leiden, opleidingen en trainingen te ontwikkelen voor gemeentelijke functies in de crisisbeheersing.

*Kristel Scheffers,  
projectleider GROOTER, adviseur Veiligheid,  
gemeente Tilburg*

Begin 2009 werkte ik als adviseur crisisbeheersing voor vier gemeenten in Brabant en was lid van een landelijk overleg. Steeds liep ik aan tegen het feit dat er voor gemeentelijke opleidingen slechts enkele opleiders beschikbaar waren. Ook waren er geen gestandaardiseerde opleidingen en trainingen voor de gemeente, waardoor ieder traject 100% maatwerk werd. Zonde van de tijd en het geld. Deze frustratie werd door mijn collega's in het landelijk overleg gedeeld. We besloten met twee anderen dat we dit zelf ook moeten kunnen. Een jaar zijn we bezig geweest om de vraag helder te krijgen. Want zo bleken om uniforme opleidingskaders te kunnen maken, ook functieprofielen nodig te zijn. Iedere gemeente en regio werkt - anders dan brand-weer, politie of GHOR - met eigen functieprofielen en draaiboeken. En we zijn zelf wel inhoudelijk deskundig, maar geen opleiders. Dat eerste jaar hebben we dan ook vooral benut om partners te zoeken, best practices te bestuderen en vooral scherp te krijgen met welke opzet we ook landelijk draagvlak konden creëren.

#### **Gewoon beginnen**

Het werd ons duidelijk dat we dat draagvlak alleen konden verkrijgen door te bouwen aan een landelijk netwerk van mensen uit het veld die hun expertise

inbrachten. Voor het veld, door het veld. Onze plannen werden door het landelijk overleg omarmd dus we gingen aan de slag. Zonder subsidie of budgetten, maar met vele enthousiaste mensen uit het hele land die zich hadden aangemeld na een oproep in het Landelijk Overleg Coördinatoren Bevolkingszorg (LOCB) en het Landelijk Overleg Coördinerend gemeentesecretarissen (LOGC). De roep om professionalisering van de gemeentelijke kolom werd in 2011 nog groter door incidenten als de brand bij Moerdijk. Tot die tijd draaiden alle deelnemers aan het project de uren op basis van vrijwilligheid en de bereidheid van hun werkgevers om tijd vrij te maken. In 2011 konden we met een subsidie van het ministerie externe ondersteuning inhuren in de vorm van projectmanagement en de Universiteit van Leiden. GROOT werd GROOTER en nam een hoge vlucht. De inzet en betrokkenheid van de leden van de expertteams bleef enorm en dat vormde, samen met de expertise van de Universiteit van Leiden een belangrijke succesfactor.

#### **80% uniform, 20% lokaal**

Een van de doelstellingen van het project was om te komen tot uniforme functieprofielen en opleidingskaders. En daar liepen we aan tegen het feit dat iedere regio anders georganiseerd is en andere fysieke

kenmerken en problemen heeft. We kwamen tot de conclusie dat 100% uniformiteit niet haalbaar is, en dat de kracht deels blijft liggen in de lokale invulling. We gaan dus voor 80% uniformiteit en 20% lokale invulling. Hierdoor wordt regionale of zelfs interregionale bijstand tussen gemeenten en veiligheidsregio's mogelijk gemaakt, en is er binnen de opleiding (en planvorming) ook ruimte voor lokaal of regionaal maatwerk.

### Weerstand overwinnen

We vonden het belangrijk om te klankborden met andere organisaties met een rol in de bevolkingszorg. Kijken waar we konden aansluiten en zorgen dat we elkaar niet doorkruisten. Vooral in het begin zorgde GROOT voor onduidelijkheid en scepticisme. 'Weer zo'n project dat niets oplevert'. Er waren opgetrokken wenkbrauwen binnen de gemeentelijke kolom, want 'wie was ik om kwaliteitseisen te stellen aan het functioneren van een gemeentesecretaris in crisistijd'. Daarnaast ondervonden we behoorlijk wat weerstand bij opleiders. De opleidingsmarkt voor crisisbeheersing is in handen van enkele opleiders die onze opleidingskaders als een bedreiging zagen. Men was bang voor broodroof en het kostte veel tijd en gesprekken voordat duidelijk werd dat GROOTER zelf geen opleidingsinstituut is of de bedoeling heeft om opleiders uit te sluiten. Nu is de teneur omgeslagen. Veel opleiders zijn betrokken of geïnteresseerd om te werken met de GROOTER producten en inmiddels hebben de eersten opleidingen ontwikkeld volgens de GROOTER-kaders. GROOTER verwordt tot een keurmerk voor professionele opleidingen. Voor ons als projectorganisatie de kers op de taart en voor de organisatie van een adequate en professionele crisisbeheersing een enorme stap voorwaarts.

### Borging bij het IFV

Inmiddels nadert het project zijn einde. We verwachten eind april van dit jaar alle opleidingskaders en functieprofielen te hebben afgerond. Het Instituut Fysieke Veiligheid (IFV) gaat zorg dragen voor de verdere borging en het beheer van de producten. Met GROOT en GROOTER is een solide basis gelegd voor een oranje kolom die volwaardig haar rol kan spelen in de crisisbeheersing. Natuurlijk is het zaak om de producten te onderhouden en verder uit te werken naargelang de ontwikkelingen in de samenleving daar om vragen. De functieprofielen vormen de basis. Deze zijn gebaseerd op competenties en vaardigheden en zullen op korte termijn niet ingrijpend wijzigen. De ontwikkeling en uitdaging zit dan ook vooral in die 20% lokale invulling. Het netwerk dat met GROOTER is ontstaan zal blijven bestaan. Het project heeft vele deuren geopend op het gebied van samenwerking. Mensen en organisaties uit

het hele land weten elkaar te vinden waar het gaat om bevolkingszorg in de crisisbeheersing en delen hun kennis. Wat mij betreft een van de grootste winsten die dit project heeft opgeleverd.

### Resultaten

- In 2012 zijn meer dan 100 Officieren van Dienst Bevolkingszorg opgeleid en geëxamineerd  
De eerste opleidingsinstituten ontwikkelden trainingen op basis van kaders GROOTER
- Landelijk netwerk op het gebied van bevolkingszorg in de crisisbeheersing
- Profielen Communicatie klaar; andere expertteams volgen de komende maanden
- Eerste proeven van bekwaamheid afgelegd
- De aanpak van GROOTER vindt internationaal navolging

Het project GROOTER won recent de Don Berghuijs Award 2012. Deze prijs, voorheen de Publieke Veiligheid Award en later genoemd naar de in 2011 overleden grondlegger van de veiligheidsregio's Don Berghuijs, werd voor de zevende keer uitgereikt en is bedoeld voor het meest innovatieve veiligheidsproject. GROOTER, gecoördineerd door de Veiligheidsregio Midden- en West-Brabant, versloeg in de finale drie andere mededingers. GROOTER wordt uitgevoerd in opdracht van het Landelijk Overleg van Coördinerend Gemeentesecretarissen. Die hebben het project in het leven geroepen om gemeenten beter toe te rusten bij hun taken op het gebied van bevolkingszorg wanneer zich een crisis of incident voordoet. Gemeenten moeten dan opereren als professionele hulpdiensten en met hun inzet naadloos aansluiten op het werk van onder andere politie en brandweer. GROOTER draagt bij aan die professionalisering door, samen met professionals uit het hele land en de Universiteit van Leiden, opleidingen en trainingen te ontwikkelen voor gemeentelijke functies in de crisisbeheersing. Het project heeft geresulteerd in uniforme opleidingskaders voor de Oranje Kolom, waarin competenties en vaardigheden centraal staan van zowel bestuurlijk strategische als operationele functionarissen op het gebied van Communicatie, ICT, secretariële ondersteuning, omgevingszorg, Opvang, verplaatsen mens en dier en Nafase.

### Meer informatie

[www.veiligheidsberaad.nl](http://www.veiligheidsberaad.nl)  
[www.ifv.nl](http://www.ifv.nl)  
[www.veiligheidaward.nl](http://www.veiligheidaward.nl)

drs. J.C.M. Netten,  
beleidsadviseur Stichting Impact  
(j.netten@impact.arq.org)  
drs. M. van de Donk,  
senior adviseur Radar Advies  
(m.vandedonk@radaradvies.nl)

# De rol van slachtoffers binnen de context van contraterrorisme

De Nederlander Max Boon wil met de actieve inzet van de stem van getroffen en lokale gemeenschappen radicalisering tegen gaan. Vanuit het International Centre of Counterterrorism (ICCT) zet hij hiervoor een organisatie op in Indonesië. Boon doet dit vanuit een bijzondere positie. Als slachtoffer van de terroristische aanslag op het Marriott-hotel in Jakarta van 2009, heeft hij aan den lijve de gevolgen van gewelddadig extremisme ondervonden.

Zijn verhaal staat niet op zichzelf. Slachtoffers van terrorisme en hun organisaties bewegen zich steeds meer op het terrein van het voorkomen van terroristisch geweld. Als - ongewenste - ervaringsdeskundigen zetten zij zich in om de samenleving of specifieke groepen te doordringen van de gruwelijke gevolgen van terrorisme.

## Inclusief stem getroffen van terrorisme

In het kader van contraterrorisme of het tegengaan van gewelddadig extremisme, zijn lokale en nationale organisaties en overheden, maar ook uiteenlopende internationale, Europese en mondiale organisaties actief. De focus lijkt niet alleen (meer) op repressie gericht te zijn, maar ook op preventie van gewelddadig extremisme en radicalisme. Nieuw is dat steeds meer

gekeken wordt welke bijdrage civic society, waaronder slachtoffers van terrorisme, hieraan kan leveren. Getroffenen van terrorisme mengden zich al langer in het publieke debat, of het nu ging om aandacht vragen voor hun rechten of om slachtoffers te gedenken. Ook was menig getroffene al betrokken bij programma's op bijvoorbeeld scholen. Het gericht werken aan bestrijding van gewelddadig radicalisme en het structureel gaan inzetten van hen is echter nieuw. De stap lijkt klein maar is groot voor de slachtoffers van terrorisme. Niet zij, niet hun verhaal maar het maatschappelijke doel staat centraal.

Op 5, 6 en 7 november 2012 vonden in Den Haag twee bijeenkomsten plaats van Europese slachtoffer(-organisaties) om deze relatief nieuwe ontwikkeling te bespreken. Centraal stond de vraag hoe en wanneer de inspanningen van slachtoffers van terrorisme effectief (kunnen) zijn.

## Counter-narratives

Het verhaal van de getroffene, de counter-narrative, moet tegenwicht bieden aan de valse heroïek en verlokkingen die radicale ideologieën kenmerken, en geeft een gezicht aan de slachtoffers. Deze counter-narratives kunnen verschillende vormen hebben: bij voorbeeld in persoon verteld voor de klas als onderdeel van een programma, of gefilmd of geschreven.

## Global Counter Terrorism Forum

Een van de initiatieven is het door Hillary Clinton in 2011 geïnstalleerde Global Counterterrorism Forum (GCTF). Het platform met 30 founding members (29 landen en de EU) brengt sleutelfiguren uit de beleids-



Impressie NAVT bijeenkomst Den Haag





*Installatie Global Counterterrorism Forum (GCTF) door Hillary Clinton (22 september, 2011)*

wereld, het veld, experts van de Verenigde Naties en andere multilaterale gremia samen. Er zijn vijf werkgroepen waaronder Countering Violent Extremism. Deze werkgroep richt zich onder andere op het tegengaan van extremistisch geweld door communicatie. Hierbij spelen instituten, scholen, gevangenis maar dus ook organisaties van getroffen van terrorisme een rol.

#### **Global Survivors Network**

In 2008 ontstond uit het 1e United Nations Symposium on Supporting Victims of Terrorism het Global Survivors Network. De stem van getroffen moest echter niet alleen binnen de VN-muren door beleidsmakers gehoord kunnen worden, maar ook door de wereld daarbuiten. Het netwerk legt sindsdien contacten met gemeenschappen die ontvankelijk kunnen zijn voor de boodschappen van extremisten. Door het creëren van momenten om tot uitwisseling van ervaringen en ideeën te komen kan er een tegengeluid, een tegestem, gehoord worden die kan bijdragen aan de-radicalisering. Het Global Survivors Network publiceert diverse getuigenissen op Internet.

#### **Europese activiteiten**

Na de grote terreuraanslagen in Europa (Madrid, Londen) is er met EU-financiering een platform, c.q. netwerk ontwikkeld van Europese organisaties van getroffen van terrorisme. Dit Network of Associations

of Victims of Terrorism (NAVt) telt meer dan 35 partners uit o.a. Spanje, Italië, Frankrijk, Engeland en Noord-Ierland. Vele NAVt-partners zetten in hun eigen land al op uiteenlopende wijzen de stem van getroffen in. Bijvoorbeeld op scholen waar zij jongeren bewust proberen te maken van de echte gevolgen van terrorisme, om hen te behoeden die weg op te gaan. Op de NAVt bijeenkomst op 5 november, die Stichting Impact als NAVt partner organiseerde, werd de mogelijke inzet van deze Voices binnen de context van contraterroerisme vanuit diverse perspectieven verkend. Bijvoorbeeld, wat weten we überhaupt over het preventief inzetten van narratives? Kunnen we hier van leren als we de getuigenissen binnen de specifieke context van contraterroerisme willen inzetten? Zo werd die dag kennis genomen van de ervaringen van het Landelijk Steunpunt Gastsprekers WO II-heden, hoe holocaustslachtoffers al sinds vele jaren effectief hun verhaal inzetten in schoolprogramma's.

Het Radicalisation Awareness Network (RAN) van de Europese Commissie brengt mensen bijeen uit de (EU-)praktijk van bestrijding van radicalisering en de-radicalisering. Eén van de werkgroepen is gewijd aan de Voices of Victims of Terrorism. Deze werkgroep houdt zich bezig met het verzamelen van methoden maar ook voorbeelden van counter-narratives. De notie is dat er al veel verhalen zijn maar vaak zijn deze nog niet ontsloten. Tevens is er nog weinig bekend over wat een verhaal effectief maakt. Tijdens de conferentie op 6 en 7 november bleek duidelijk dat aard en cultuur van de doelgroep erg belangrijk zijn voor ontvankelijkheid voor de boodschap.

TERRA (Terrorism and Radicalisation) is een ander Europees project dat medio 2012 gestart is, en dat Impact coördineert. Doel is onder andere het kritisch denken en bewustzijn bij jongeren te vergroten rondom radicalisering en terrorisme, en ook slachtoffers van terrorisme te ondersteunen in het ontwikkelen van positieve counter-narratives, en zo contraterroerisme te versterken.

#### **Van indrukwekkend naar effectief**

Tijdens de NAVt- en RAN-bijeenkomst vertelden overlevenden van aanslagen en nabestaanden over hun ervaringen in relatie tot het thema contraterroerisme. Indringende, bijzondere, ontroerende en moedige, verhalen, die ook inspireren en je stil maken. De motivatie van getroffen om bij te dragen aan de strijd tegen gewelddadig radicalisering is groot, maar niet algemeen. Sommigen kiezen ervoor om niet met hun verhaal naar buiten te treden. De groep die zich wel wil en kan inzetten verzet nu al veel werk. De uitdaging voor komende periode is om met hen te kijken hoe de krachtige stem van getroffen zo effectief mogelijk in te zetten.

**Wouter Botzen,**

universitair docent Milieueconomie

**Jeroen Aerts,**

hoogleraar Klimaatrisico's, waterbeheer en verzekeringen

**Hans de Moel,** onderzoeker Overstromingsrisico's en waterbeheer

Allen verbonden aan de Vrije Universiteit Amsterdam, Instituut voor Milieuvraagstukken

# Superstorm Sandy

## Getrokken lessen en een Nederlandse aanpak in New York City

Orkaan Sandy heeft eind vorig jaar veel New Yorkers eraan herinnerd dat zij in een gebied wonen dat getroffen kan worden door zware orkanen die grootschalige overstromingen kunnen veroorzaken. De substantiële economische schade en maatschappelijke ontwrichting als gevolg van orkaan Irene in 2011 (Aerts en Botzen, 2012a) en meer recentelijk van orkaan Sandy hebben ervoor gezorgd dat een betere preventie en beheersing van overstromingsschade een belangrijk onderwerp op de politieke agenda is geworden. Ondanks succesvolle evacuaties van ongeveer 370.000 mensen eiste orkaan Sandy 41 slachtoffers in New York City. De schade in de stad aan gebouwen, infrastructuur en de economie bedroeg enkele tientallen miljarden dollars. Het openbare leven in New York raakte ernstig verstoord doordat miljoenen huishoudens zonder stroom kwamen te zitten en het openbaar vervoer niet meer goed kon functioneren vanwege beschadigingen aan treinrails en ondergelopen metrotunnels. Een gevolg hiervan was dat vitale economische activiteiten enkele dagen stillagen, zoals de New York Stock Exchange.

De verwachting is dat zonder een verbetering van het waterbeheer overstromingsrisico's in New York City substantieel kunnen toenemen door twee ontwikkelingen die dit risico op de lange termijn beïnvloeden. Een analyse van de ontwikkeling van de waarden van gebouwen in overstroombare gebieden in New York City vanaf 1880 tot 2010 toont aan dat deze waarden elk jaar gestaag zijn toegenomen (Aerts en Botzen, 2012b). Projecties van bevolkingsgroei en economische ontwikkelingen in New York duiden erop dat de komende decennia deze waarden die blootgesteld zijn aan overstromingen verder zullen stijgen. Daarnaast is de verwachting dat klimaatverandering en de daarmee gepaarde zeespiegelstijging zal leiden tot hogere waterstanden tijdens overstromingen en mogelijk een toename in de kans op zware orkanen als gevolg heeft.

Voor het formuleren van beleidstrategieën voor het beperken van overstromingsrisico's in New York is het van belang om goede inzichten te hebben in dit risico. Hiervoor heeft de Vrije Universiteit het overstromingsrisico in New York City in detail in kaart gebracht (Aerts e.a., 2013). In dit onderzoek is voor 214 zware stormen berekend welke gebieden in de stad kunnen overstromen en hoe hoog de verwachte waterdieptes in die

gebieden zullen zijn. Vervolgens is met behulp van een schademodel en gedetailleerde ruimtelijke informatie van de waarde van bestaande gebouwen in New York de verwachte directe schade aan gebouwen voor elk van deze 214 stormen berekend. De resultaten tonen aan dat overstromingsschade aan gebouwen tussen de \$2-5 miljard bedraagt voor een stormvloed met een kans van 1/100 en tussen de \$5-11 miljard voor een stormvloed met een kans van 1/500, terwijl deze schade kan oplopen tot \$26 miljard voor zeer zware stromen (Aerts e.a., 2013). Hierbij dient te worden opgemerkt dat deze resultaten alleen directe schade aan gebouwen betreffen, en dus geen schade aan infrastructuur en indirecte – economische – schade (bedrijfsuitval) bevatten waardoor de totale overstromingsschade substantieel hoger zal uitvallen. Een ruimtelijke analyse van het risico laat zien welke gebieden van New York City het grootste risico lopen en waar maatregelen dus geprioritiseerd dienen te worden. Relevant voor beleid is tevens de bevinding dat een groot gedeelte van de schade (tussen de 14-40%) buiten de gebieden kan plaatsvinden die door de "Federal Emergency Management Agency" (FEMA) zijn aangewezen als overstromingszone.

De toekomstige houdbaarheid van het beleid ten aanzien van overstromingsrisico's in New York City is geanalyseerd (Aerts en Botzen (2011). Schadebeperkende maatregelen door middel van bouwvoorschriften hebben een centrale rol in het huidige beleid dat ten opzichte van Nederland minder gericht is op preventie van overstromingen. Een belangrijke pijler voor waterbeheer in Amerika is het federale nationale verzekeringsprogramma voor overstromingsschade die bouwvoorschriften vaststelt voor nieuwbouw in gebieden die volgens FEMA een overstromingskans hebben van 1/100. Een voorbeeld hiervan is het ophogen van woningen tot aan het verwachte waterniveau dat kan worden bereikt tijdens een overstroming. New York City stelt extra eisen voor ophoging van vitale infrastructuur en gebouwen met een belangrijke maatschappelijke functie, zoals ziekenhuizen, maar deze extra eisen gelden niet voor residentiële gebouwen. Deze mix van beleidsmaatregelen – gericht of het beperken van potentiële overstromingsschade en het

vergoeden van zulke schade door verzekeringen – kan interessante aanknopingspunten verschaffen voor het Nederlandse waterbeheer waarin “meerlaagse veiligheid” een belangrijk thema is geworden, ofwel verder kijken dan alleen preventie.

Uit de ervaringen met orkaan Sandy en recente onderzoeksresultaten kunnen enkele belangrijke lessen worden getrokken voor het ontwikkelen van beleid om de kans en mogelijke schade van toekomstige overstromingen in New York City te beperken. De discussie hierover richt zich enerzijds op het aanscherpen van het huidige beleid van bouwvoorschriften en ruimtelijke ordening om overstromingsschade te reduceren of anderzijds op investeringen in stormvloedkeringen en dijkinfrastructuur om de kans op zware overstromingen te verkleinen. Zoals is beschreven in het onderzoek uit 2011 kan schadepreventie o.a. worden verbeterd door:

1. bouwvoorschriften op te stellen voor gebouwen in gebieden buiten de officiële 1/100 FEMA overstromingszones waar volgens analyses wel degelijk een reëel overstromingsrisico bestaat; (2) rekening te houden met lange termijn risico's in bouwvoorschriften, zoals extra eisen voor ophoging van nieuwbouw vanwege verwachte zeespiegelstijging;
2. extra eisen te stellen aan het ophogen van residentiële gebouwen die een groot gedeelte van de schadelast veroorzaken, zoals nu al gebeurt voor gebouwen met een belangrijke maatschappelijke functie;
3. goedkopere methodes dan ophoging te onderzoeken om bestaande gebouwen tijdens reeds geplande renovaties beter bestendig te maken tegen overstromingen;
4. met ruimtelijke ordening bebouwing in relatief veilige gebieden te stimuleren.

Zoals bleek uit de ervaringen met orkaan Sandy is het van belang om in dit beleid prioriteit te geven aan vitale infrastructuur, zoals bescherming van het metrosysteem. Een nadeel van het aanscherpen van het huidige bouwvoorschriften beleid is dat het de kans op overstromingen en de daarmee gepaarde ontwrichting van de lokale economie niet reduceert. Geïnspireerd op het Nederlandse watersysteem, wordt er in New York dan ook discussie gevoerd over het plaatsen van stormvloedkeringen en dijken om de stad te beschermen tegen toekomstige orkanen en stormvloed (Aerts en Botzen, 2012c). Een lastig obstakel is of de zeer grote investeringskosten hiervan die tussen de 15-25 miljard euro liggen politiek te verantwoorden zijn in tijden van fiscale crisis van de Amerikaanse overheid. Orkaan Sandy heeft ervoor gezorgd dat ook deze politiek moeilijk haalbare maatregelen een reëel beleidsalternatief zijn geworden.

## Referenties

- Aerts, J.C.J.H. en Botzen, W.J.W. (2011), 'Climate-resilient waterfront development in New York City: Bridging flood insurance, building codes, and flood zoning', in: *Annals of the New York Academy of Sciences*, 1227: 1-82.
- Aerts, J.C.J.H. en Botzen, W.J.W. (2012a). Hurricane Irene: A wake up call for New York City? *Natural Hazards and Earth System Sciences*, 12: 1837-1840.
- Aerts, J.C.J.H. en Botzen, W.J.W. (2012b), 'Managing exposure to flooding in New York City (NYC)', in: *Nature Climate Change*, 2: 377.
- Aerts, J.C.J.H. en Botzen, W.J.W. (2012c). 'Climate adaptation cost for flood risk management in the Netherlands' in: D. Hill, M.J. Bowman en J.S. Khinda (eds), *Storm Surge Barriers to Protect New York City: Against the Deluge*. American Society of Civil Engineers (ASCE), Reston, 99-114.
- Aerts, J.C.J.H., Lin, N., de Moel, H., Emmanuel, K. en Botzen, W.J.W. (2013), 'Lowprobability flood-risk modeling for New York City', in: *Risk Analysis* (In druk).



Een tool om gezamenlijk sneller en transparanter te besluiten

# Afwegingsinstrument Veiligheid en Economie

Bij besluitvorming op het terrein van veiligheid is ondersteuning door meer kwantitatieve methodes eerder uitzondering dan regel. En als dat gebeurt, dan wordt het uitbesteed aan externe bureaus. Dit vergt echter veel tijd en geld, wat niet altijd beschikbaar is: de hoofdreden waarom er vaak van wordt afgezien.

*dr. J. van der Knoop,  
Decide, verbonden  
aan de Rijksuniversiteit  
Groningen en de  
dutch group  
dr. H.C.J. van der Veen,  
Wetenschappelijk  
Onderzoek en  
Documentatie-  
centrum (WODC),  
Ministerie van  
Veiligheid en Justitie*

In deze bijdrage wordt een generiek afwegingsinstrument gepresenteerd dat gratis beschikbaar is, snel tot resultaten leidt en dat door beleidsfunctionarissen zelf kan worden toegepast, wat ook nog een leereffect geeft. Het instrument is in twee veiligheidsstudies succesvol getest. Het biedt besluitvormers een structuur voor het waarderen van verschillende keuzes in besluitvormings-situaties. Het vergemakkelijkt de argumentatie voor de 'beste' keuzes, zodat deze beter kunnen worden verantwoord.

De keuze van de meest adequate veiligheidsmaatregelen is om meerdere redenen complex. Om te beginnen zijn de effecten van de diverse maatregelen vaak onzeker. Verder spelen naast veiligheid andere afwegingscriteria een rol, zoals kosten, waarbij de afweging tussen veiligheid en kosten erg lastig is. Ook is de uitkomst vaak afhankelijk van het perspectief van de partij die de afweging maakt. Beleidsmakers zijn daarom erg gebaat bij kwantitatieve tools die rekening houden met dergelijke lastige aspecten en die bovendien snel en goedkoop inzetbaar zijn. In deze bijdrage wordt zo'n instrument gepresenteerd.

## Ontwikkeling

Decide ontwikkelde in opdracht van het WODC het 'Afwegingsinstrument Veiligheid en Economie' (AVE) in 2008 met het doel de kwaliteit en efficiency van de besluitvorming op het gebied van sociale veiligheid te verhogen. Uitgangspunten waren: eenvoud - de gebruiker moet het zelf kunnen toepassen -, brede inzetbaarheid - geschikt voor diverse besluitvormings-situaties -, transparantie - afwegingen expliciteren -, snelheid en lage kosten.

AVE is een speciale vorm van multicriteria-analyse. Het biedt de mogelijkheid verschillende veiligheidsmaatregelen tegen elkaar af te wegen. Het werd in acht cases

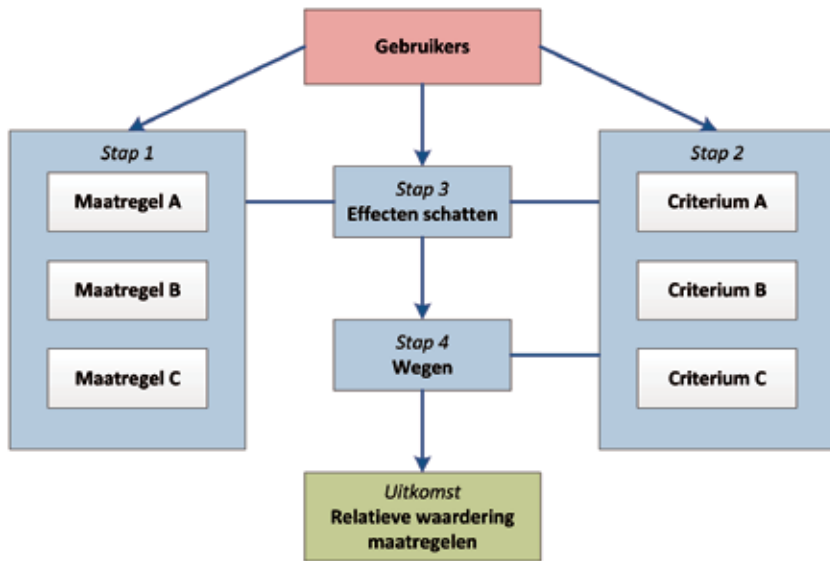
getest, meest bij maatregelen ter verbetering van de veiligheid in winkelcentra of wijken. De gebruikers beoordeelden AVE zeer positief.

In 2012 gaf het WODC op verzoek van de afdeling Generieke Veiligheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid opdracht AVE op toepasbaarheid te toetsen bij besluiten over fysieke veiligheid. Dit leidde tot het rapport Toepassing van een vereenvoudigd afwegingsinstrument bij keuzes op het terrein van fysieke veiligheid (Decide, 2012). In het kader van dit onderzoek toetste de Brandweer Midden- en West Brabant AVE in twee cases. Bij beide was het doel na te gaan welke maatregelen het beste genomen kunnen worden ter compensatie van het niet voldoen aan de norm voor de maximale opkomsttijd van de brandweer (in het kader van het Besluit Veiligheidsregio's). De eerste casus betrof een zorgcentrum en de tweede een heel dorp. In beide gevallen werd de maximale opkomsttijd zeker overschreden. Ook hier waren de gebruikers enthousiast en passen ze inmiddels AVE zelf toe. Aan de hand van de casus over het zorgcentrum wordt in deze bijdrage de toepassing van AVE kort toegelicht.

## Toepassing

De eerste vraag met betrekking tot het zorgcentrum was welke compenserende maatregelen beschikbaar waren (Stap 1). Men overwoog onder andere de aanleg van een sprinklerinstallatie, een versterking van de Bedrijfshulpverlening (BHV), een verbeterde preparatie van de brandweer, het stimuleren van het brandveilig gebruik van het gebouw, het oefenen van BHV en bewoners te zamen en maatregelen ter verkorting van de opkomsttijd. Alle maatregelen, in totaal acht, werden zoveel mogelijk gespecificeerd.

Vervolgens werd een lijst opgesteld van twaalf criteria aan de hand waarvan men de maatregelen wilde evalueren of vergelijken (Stap 2). De leidende vraag hierbij is: waaraan weeg ik de effectiviteit van de maatregelen af? Dat zijn uiteraard effecten op veiligheidscriteria zoals 'de kans op het ontstaan of op uitbreiding van brand', 'de opkomsttijd van de brandweer', 'de inzettijd van de brandweer' en 'de effectiviteit van de BHV'. Daarnaast werden andersoortige criteria opgenomen zoals 'kosten (direct en structureel)', 'beslag op het personeel van de brandweer' en 'implementatiemoeilijkheid'.



Figuur 1: Stappen bij toepassing van AVE

Daarna werden de effecten van elk van de maatregelen op elk van de criteria geschat (Stap 3). Dit gebeurde in een groepsessie waaraan, naast deskundigen van de brandweer, ook vertegenwoordigers van de gemeente en de eigenaar van het zorgcentrum deelnamen. In onderlinge discussie werden 'effectscores' toegekend aan de verwachte effecten van de overwogen maatregelen op de criteria. Het gaat om scores op algemene schalen en de maatregelen worden aan de hand hiervan vergeleken op hun effecten op de criteria. Omdat het gewicht van de criteria kan verschillen, werd vervolgens een weging toegepast op de verschillende effecten (Stap 4). Zodoende weegt het effect op een belangrijk criterium zwaarder dan het effect op een minder belangrijk criterium. Deze weging hoeft niet voor alle personen gelijk te zijn, bijvoorbeeld vanwege verschillen in hun belangen. Daarom staat AVE

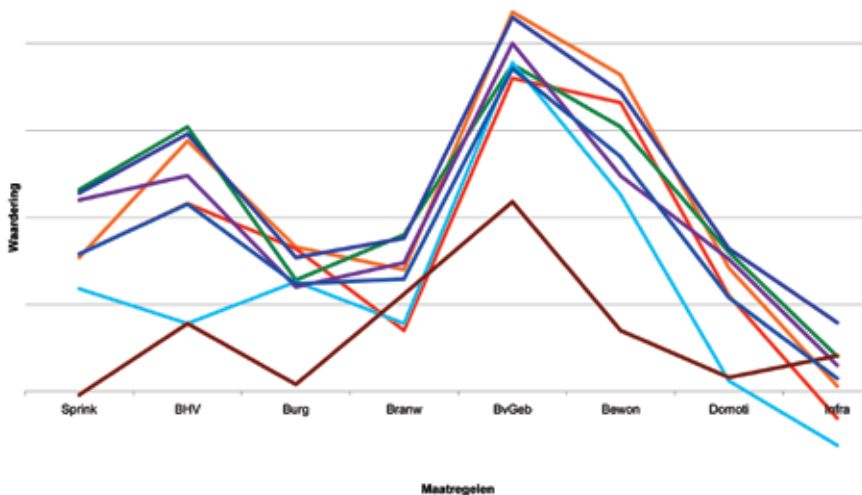
individuele wegingen toe voor alle deelnemers aan de sessie. Ten slotte berekent AVE de uitkomst: een rangorde in de keuzealternatieven op basis van de hoogte van de waardering van de maatregelen. In figuur 1 worden de stappen schematisch weergegeven.

Figuur 2 is een grafische weergave van de analyse-uitkomst voor de beschreven casus. Op de horizontale as staan de labels van de maatregelen. De verticale as geeft de hoogte van de waardering weer. Elke lijn verbindt de waarderingsscores van een deelnemer aan de groepsessie. Het patroon in de figuur maakt inzichtelijk dat de waarderingen van de maatregelen voor de meeste deelnemers weliswaar leiden tot verschillende scores, maar ook dat hun rangordering van de maatregelen in belangrijke mate gelijk uitpakt. Dit geldt zeker voor de drie hoogst en de drie laagst gewaardeerde maatregelen. Veel van de andere onderzochte casus leiden eveneens tot een dergelijke uitkomst.

Figuur 2 laat zien dat in de casus de maatregelen die waren gericht op het verbeteren van het gedrag van bewoners en BHV - preventief en reactief op brand - het hoogst scoorden. Het gaat om 'Versterking van de BHV' (in de figuur gelabeld als BHV), 'Stimulering brandveilig gebruik gebouw' (BvGeb) en 'Het oefenen van BHV en bewoners' (Bewon). Daarentegen scoorden maatregelen die de opkomsttijd verkorten bij bijna alle deelnemers het laagst (Infra). Dit is opmerkelijk gezien het gewicht dat de politiek aan de opkomsttijd geeft.

### Evaluatie

AVE brengt een rangorde aan naar waardering van de gebruikers op basis van een veelheid aan criteria. De meerwaarde van AVE is ten eerste de structurering van de besluitvorming als proces en de versnelling ervan. Ten tweede dat het afwegingsproces gezamenlijk wordt gedragen door de deelnemers. Daarnaast dient AVE de transparantie doordat argumenten expliciet worden gemaakt. Een ander belangrijk voordeel is dat zeer diverse effecten, zoals veiligheid en kosten, in de analyse geïntegreerd worden. Toepassing kost weinig tijd; zo nodig kan de exercitie in drie uur worden uitgevoerd. Dit maakt AVE ook geschikt voor besluiten die onder tijdsdruk moeten worden genomen. De afdeling Generieke Veiligheid van de NCTV is tevreden met het resultaat en wil de toepassing van AVE bevorderen. Alvorens AVE zelf toe te passen is het aanbevelenswaardig de rapporten te lezen, te oefenen met AVE of begeleiding te vragen van iemand die ervaring heeft in het gebruik ervan. AVE is gratis beschikbaar en is, evenals de twee rapporten, te downloaden via de website van het WODC: [www.wodc.nl](http://www.wodc.nl).



Figuur 2: Uitkomsten afweging compenserende maatregelen zorgcentrum



# Gaan sociale media 1-1-2 vervangen?

Het lijkt een ontwikkeling te zijn waar we niet meer om heen kunnen: het gebruik van sociale media bij noodsituaties door burgers en hulpdiensten. Maar wat verwachten burgers nu met betrekking tot het gebruik van sociale media door hulpdiensten tijdens noodsituaties? Verwachten burgers inmiddels dat sociale media zijn in te zetten tijdens noodsituaties, of is dat nog een brug te ver? Of zijn sociale media op termijn misschien een vervanging voor 1-1-2? Zeker nu de bereikbaarheid van 1-1-2 ook opnieuw ter discussie is gesteld. 100% bereikbaarheid is namelijk niet te garanderen voor het alarmnummer 1-1-2.

## Onderzoek

In de zomer van 2012 voerde adviesbureau VDMMP in samenwerking met lector crisisbeheersing Menno van Duin een onderzoek uit naar bovenstaande vragen. Een tweede onderzoek volgde kort hierop. Bij beide onderzoeken vulden ruim duizend respondenten de vragenlijst volledig in, in totaal dus meer dan tweeduizend ingevulde enquêtes. De resultaten van beide onderzoeken geven daarmee een goede indicatie van de verwachtingen van burgers met betrekking tot het gebruik van sociale media tijdens noodsituaties.

## Zelfredzame burger op sociale media

Uit de onderzoeksresultaten blijkt dat burgers zelfredzaam zijn en willen zijn; ook op sociale media. Zo verwacht 50.6% (NB: alle getallen zijn een gemiddelde op basis

van beide onderzoeken) van de respondenten sociale media (met name Twitter en Facebook) in te zetten bij een noodsituatie om familie en vrienden te laten weten dat ze veilig zijn. Ook geeft 50.2% van de respondenten aan eigen waarnemingen van noodsituaties op sociale media te plaatsen. Respondenten verwachten een hulpvraag qua acute gezondheidszorg of primaire levensbehoeften op sociale media te plaatsen voor zichzelf (42.8%) of voor de medemens (50.0%).

## Hulp(diensten) op de sociale media

Het merendeel van de burgers verwacht van de hulpdiensten dat zij sociale media 24/7 monitoren en dat zij direct reageren op hulpvragen die via sociale media gesteld worden. 43.3% van de respondenten verwacht dat over vijf jaar de reactie van de

hulpdiensten op een melding via sociale media even snel is als de reactie op een melding die via 1-1-2 wordt gedaan. Daarnaast verwacht een meerderheid van de respondenten (79.8%) sociale media te gebruiken om de hulpdiensten te bereiken als het telefoonnetwerk niet werkt.

## Conclusie

Sociale media worden nu al gebruikt door burgers bij noodsituaties en dit lijkt in de toekomst alleen maar meer te worden. Zeker als het telefoonnetwerk niet werkt, verwacht het merendeel van de burgers sociale media in te zetten. Sociale media blijken al een volwaardig communicatie-instrument naast bellen en sms'en. Onder meer na de storm Sandy zijn diverse hulpvragen via Twitter en Facebook gedeeld met de buitenwereld. Echter als het (mobiel) internet eruit ligt dan is het afgelopen met communiceren op en via de sociale media. Kortom: ook hier is sprake van een kwetsbaarheid, en lijkt ook 100% garantie niet mogelijk. Sociale media lijken dus op korte termijn 1-1-2 niet zozeer te gaan vervangen, maar kunnen wel als een waardevolle aanvulling beschouwd worden, of in elk geval als een soort back-up-systeem bij noodsituaties. Meer informatie en een samenvatting van beide onderzoeken zijn te vinden op [www.vdmmp.nl](http://www.vdmmp.nl)<sup>1</sup>.



Foto: Arthur Wijnen

<sup>1</sup> <http://vdmmp.nl/nieuwsarchief/289-gaan-sociale-media-over-vijf-jaar-1-1-2-vervangen-.html>

# Colofon

## Redactieadres Magazine nationale veiligheid en crisisbeheersing

Ministerie van Veiligheid en Justitie  
Kamer H1849  
Postbus 20301  
2500 EH Den Haag  
E-mail: [magazine@nctv.minvenj.nl](mailto:magazine@nctv.minvenj.nl)  
Internet: [www.nctv.nl](http://www.nctv.nl)

## Redactiecommissie

Esther de Kleuver, Chris van Duuren,  
Arjo van Driel, Chris Hanekamp,  
Hedzer Komduur, Martine van de Kuit,  
Jan-Bart van Oppenraaij,  
Eelco van Stofbergen, Maaïke van Tuyl  
en Geert Wismans (samenstelling en  
eindredactie)

## 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. Michel van Eeten (Technische Universiteit Delft)  
Prof. dr. Georg Frerks (Universiteit Wageningen)  
prof.dr. Beatrice de Graaf (Universiteit Leiden/Centre for Terrorism & Counterterrorism)  
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 (Universiteit Leiden, The Hague Centre for Strategic Studies)

## Aan dit nummer werkten mee:

Jelle van Aanholt, Jeroen Aerts, Niek van As, Marjolein van Asselt, Tuba Avdan, Frank Bacco, Gunnar Bakker, Krijn van Beek, Peter de Beijer, Jan Bos, Wouter Botzen, Barbara Clasie, M. van de Donk, Menno van Duin, Patrick van der Duin, Sandro Etalle, Elize Fallon, Wim van Geloven, Arjen Gerritsen, Nicole Groen, Hans Hazebroek, Marijke van Hees, A. Hijmering, Michiel Hoorweg, Roy Johannink, Nico Kaptein, Jelle Keuning, But Klaasen, Wim Klijn, J. van der Knoop, Henk Kool, Maurits Kreijveld, Judith van Krieken, Paul Kruis, Gert-Jan Ludden, Marco Meesters, Hans de Moel, Edmée Moojen, Mohamed Mouch, Roelof Muis, Josée Netten, Jan-Bart van Oppenraaij, Matthijs Paf, Jacqueline Roig, Kristel Scheffers, Aart Jan Smits, Mark van Staalduinen, Alies Struijs, Fanny de Swarte, Henk van der Veen, Peter de Vries, Ilona van der Vegte-Zoete, Stéphanie de Vroet, Leo Zaal, Fred Zaaijer, Peter van Zanten, Boukje van der Zee

## Fotografie

ANP, Arthur Wijnen Photography, CEG, Sandro Etalle, Defensievoorzichting, Gemeente Den Haag, IFV, Nationale Beeldbank, NCTV, Bert Spiertz, TNO

## Illustraties

GHOR Nederland, SIS, WODC

## Cartoons

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  
J-16978

## Druk

DamenVanDeventer

© Auteursrecht voorbehouden.  
ISSN 1875-7561

Voor een gratis abonnement mail: [magazine@nctv.minvenj.nl](mailto:magazine@nctv.minvenj.nl)  
Het magazine is te downloaden via [www.nctv.nl](http://www.nctv.nl)

# Vier vragen aan:



Leo Zaai,  
algemeen directeur Instituut Fysieke Veiligheid (IFV)

## Wat wilt u bereiken met het Instituut Fysieke Veiligheid?

“Met de oprichting van het Instituut wil ik een bijdrage leveren aan het verbeteren van de (fysieke) veiligheid in Nederland. Door de samenvoeging van vijf bestaande organisaties wordt de onderlinge samenwerking versterkt en ontstaat er meer synergie. Vanuit deze synergie levert het IFV in één instituut hoogstaande expertise, kennis en onderzoek, waarmee de veiligheidsregio's worden ondersteund. Het IFV wil in hecht netwerkverband samenwerken met de veiligheidsregio's aan het uitvoeren van gemeenschappelijke activiteiten op het terrein van de rampenbestrijding en crisisbeheersing. Samen met de veiligheidsregio's wordt de prioriteitenagenda opgesteld, van waaruit de activiteiten van het IFV worden afgeleid. Daarnaast mogen de veiligheidsregio's verwachten dat het IFV vanuit haar expertise ook suggesties voor vernieuwing aandraagt.”

## Wat is de link tussen innovatie en het IFV?

“Het IFV is van en voor de veiligheidsregio's. Een wens van de veiligheidsregio's is meer aandacht voor innovatie, zodat blijvend ingespeeld kan worden op snelle maatschappelijke veranderingen en technologische vernieuwingen. Innoveren heeft daarbij de focus op verbeteren, maar dan wel vanuit een grote betrokkenheid met de vraag uit het veld! Het gaat over het introduceren van vernieuwingen die nuttig zijn. Bij effectief innoveren is de centrale vraag: kan het veiligheidsoptreden slimmer, goedkoper, robuuster of duurzamer? Veel mensen denken dan

al snel aan technologie. Maar je kunt ook processen anders organiseren (out of the box) of specifieke plekken in de organisatie versterken. Voorop staat dat als we willen vernieuwen, dit een activiteit is die aandacht en inzet nodig heeft. Innoveren is ook een kwestie van doen!

De prioriteitenagenda van het Veiligheidsberaad is leidend voor de programma's die de komende jaren binnen het IFV worden uitgevoerd. Het is nadrukkelijk de bedoeling om daarbij een focus aan te brengen op vernieuwing. De thema's in de prioriteitenagenda gaan over 'de juiste dingen doen'. Bij de uitwerking zal de nadruk moeten komen te liggen op het 'goed doen'.”

## Wat vindt u de belangrijkste innovatieve uitdaging op het terrein van (fysieke) veiligheid?

“Naast de uitdaging om innovatief denken tot in de haarvaten van het IFV vorm te geven is het onderwerp netcentrisch werken een mooi voorbeeld van hoe innovatie leidt tot verandering en verbetering. Gekomen vanuit Defensie dwingt de netcentrische werkwijze de veiligheidsregio's, en daarmee ook het IFV, tot innovatief denken op het gebied van informatiedeling, leiderschap en besluitvorming tijdens rampen en crises. Innovatie speelt echter ook een cruciale rol bij het beheer en de doorontwikkeling: voortdurend moet het IFV zich afvragen hoe de samenwerkingspartners nog beter ondersteund kunnen worden en waar dit slimmer, beter of goedkoper kan. Ik denk daarom dat de belangrijkste innovatieve uitdaging twee kanten heeft. Enerzijds

de uitdaging voor het IFV om samen met de veiligheidsregio's de netcentrische werkwijze door te ontwikkelen en het proces informatiemanagement verder te professionaliseren. Anderzijds de uitdaging om het samenspel tussen het IFV en de veiligheidsregio's (als belangrijkste partner in deze) soepel te laten verlopen, met respect en aandacht voor elkaars taken en verantwoordelijkheden.”

## Hoe kunnen wij in Nederland onze innovatieve krachten beter benutten op het terrein van fysieke veiligheid?

“Met het onderbrengen van verschillende organisaties binnen het IFV ontstaat er meer ruimte voor vernieuwing en innovatie. De organisatie groeit naar circa 250 medewerkers, wat een enorm potentieel aan ervaring en ideeën oplevert. Deze beweging is mooi, maar niet voldoende. Voor echte innovaties in het veiligheidsdomein is het belangrijk dat het IFV ook haar vensters opent naar de buitenwereld en naar 'zusterorganisaties' in het veld. Daarbij denk ik aan de Politie Academie, aan TNO, het Nederlands Forensisch Instituut, het Haags Centrum voor Strategische Studies (betrokken bij de ontwikkeling van de Haagse Security Delta) en aan verschillende universiteiten in binnen- en buitenland. Maar ook Defensie (inclusief haar opleidingsinstituut) is voor meer innovatie een belangrijke speler! Innovaties ontstaan meestal wanneer je met elkaar werkt aan het verbeteren van een vraagstuk waar je in principe niet zelf uitkomt en bent aangewezen op de hulp van anderen. Die samenwerking geeft energie en daarbij mogelijkheden.”

<sup>1</sup> De volgende organisaties zijn opgegaan in het IFV: Nederlands Instituut Fysieke Veiligheid, Bureau Veiligheidsberaad, Bureau Brandweer Nederland, Landelijke Faciliteit Rampenbestrijding (LFR) en Nederlands bureau brandweereexamens (Nbbe).