Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

the way we see it

Trends in Veiligheid 2010

Samen werken aan veiligheid

Trends in Veiligheid 2010

Samen werken aan veiligheid

Capgemini Nederland B.V.

Utrecht, september 2010

Voorwoord

Sinds de aanslagen in New York en Washington op 9/11 staat het thema Veiligheid hoog op de politieke en bestuurlijke agenda's. Veiligheid is populair, krijgt veel aandacht in de media en staat centraal in een aantal recente ontwikkelingen in het politieke, economische en maatschappelijke landschap. Een groot aantal overheidsinstanties speelt actief in op deze ontwikkelingen en zorgt voor een rijke schakering aan initiatieven in de keten van openbare orde en veiligheid.

Een aantal van deze initiatieven en vernieuwingen vindt echter geïsoleerd van elkaar plaats of heeft een sterk lokaal karakter. Enerzijds worden hiermee oplossingen gecreëerd, passend bij de keuzes die we maken bij de inrichting van de besturing van de organisaties die actief betrokken zijn bij publieke veiligheid. Anderzijds plaatst het ons ook voor dilemma's. Immers, kwaadwillende elementen trekken zich weinig aan van grenzen of regelgeving en verleggen hun werkterrein razendsnel als de omstandigheden hen daartoe dwingen.

Het is van toenemend belang dat er op het snijvlak van vrijheid en veiligheid optimaal wordt samengewerkt tussen de betrokken organisaties in het veiligheidsdomein. Dit vraagt om tijdige coördinatie, effectieve uitwisseling van informatie en vooral om de bereidheid kennis en informatie te delen. Alleen op die manier kan dreigend gevaar tijdig worden onderkend en afgewend.

Het vraagt ook om leiderschap, vertrouwen en de ontwikkeling van een strategische visie. Op basis daarvan kan worden gewerkt aan zaken zoals: de vorming van eenduidiger beleid, de harmonisatie van processen en het standaardiseren van belangrijke bouwstenen. Iets waar we graag aan meewerken.

Capgemini is al jaren zowel nationaal als internationaal actief op het gebied van openbare orde en veiligheid (OOV). Wij adviseren overheden en maatschappelijk betrokken organisaties op het gebied van strategische en organisatorische innovaties. We onderzoeken de impact van maatschappelijke trends en technologische ontwikkelingen en bouwen aan oplossingen om samenwerking - in de meest brede zin van het woord - te bevorderen. Vanuit deze ervaringen hebben wij dit eerste rapport Trends in Veiligheid geschreven. Het vormt een overzicht van de belangrijkste ontwikkelingen in de OOV-sector en onze visie daarop. Waar liggen de kansen? Hoe kom je tot verantwoorde innovaties? En hoe voorkom je dat OOV-beleid wordt gemaakt op basis van krantenkoppen?

We geven u onze inzichten en onze ideeën en nodigen u van harte uit hierop te reageren via www.capgemini.nl/veiligheid. Want grensverleggende inzichten en intelligente oplossingen komen uiteindelijk altijd tot stand dankzij constructieve samenwerking en dialoog.

Drs. Geert de Vet
Vice-President Veiligheid Capgemini

Inhoudsopgave

Inleiding Trends in Veiligheid

Met deze eerste editie van Trends in Veiligheid zet Capgemini de toon voor een dialoog over veiligheid in Nederland. We doen dat op een pragmatische manier, om een beweging op gang te brengen. Het doel is daarbij niet om een waardeoordeel te geven over inspanningen uit het verleden, maar uitdagingen te schetsen waar Nederland de komende jaren voor staat. In een steeds verder globaliserende wereld lijken de relaties tussen landen, stromingen, geloofsovertuigingen en mensen steeds complexer. Om grip te krijgen op deze complexiteit is samenwerking noodzakelijk. Samenwerking tussen landen, waarover u kunt lezen in het hoofdstuk 'Europa, sta op en maak de wereld veiliger!', maar ook betere samenwerking tussen organisaties in Nederland.

De laatste jaren is ook in het veiligheidsdomein een grote variëteit van organisaties van elkaar afhankelijk. Naast de gebruikelijke hulpverleningsdiensten, ministeries en inlichtingendiensten zien we een toename van hulpstructuren en coördinerende organisaties. In het hoofdstuk 'Bestuurlijke aanpak van georganiseerde misdaad in Nederland' staan we stil bij nieuwe samenwerkingsvormen om de georganiseerde misdaad te bestrijden vanuit een bestuurlijk-preventieve invalshoek.

Samenwerking staat ook centraal in het hoofdstuk 'Veiligheidshuizen: bureaucratische theekrans of doelmatige coördinatie!?'. Hierbij wordt ingegaan op vier gouden regels om optimaal gebruik te maken van deze samenwerkingsvorm tussen bestuurlijke, strafrechtelijke en zorginstellingen. Een van de grootste valkuilen bij het organiseren van samenwerking wordt gevormd door het gebrek aan vertrouwen. De structuren en formele afspraken kunnen nog zo helder zijn, als het persoonlijke vertrouwen ontbreekt is de samenwerking een farce. Dit geldt ook voor netcentrisch werken waarbij het delen van informatie cruciaal is. In het hoofdstuk 'Beter functioneren door in anderen te investeren' wordt ingegaan op het halen versus brengen en op het investeren versus oogsten: waar ligt de balans?

Nederland is bij uitstek een land dat de voordelen van de globalisering benut. Met onze diepgewortelde handelsgeest zien wij de open grenzen en onze rol op het internationale toneel dan ook als vanzelfsprekend. Het zijn factoren die van oudsher een belangrijke bijdrage aan onze welvaart hebben gehad. Tegelijkertijd hebben onze rol in de wereldhandel, de relatief overgedimensioneerde infrastructuur en onze stellingname in zaken als recht en onrecht in de wereld, ook een aanzuigende werking op ellende. Onze open maatschappij biedt mogelijkheden voor mensen met kwade bedoelingen. Niet alleen met conventionele middelen, ook in 'cyberspace'. Het hoofdstuk 'Ter land, ter zee, in de lucht en op het web' maakt dat pijnlijk duidelijk.

In de loop van de geschiedenis heeft Nederland zich ontwikkeld tot een internationaal gerichte, multiculturele samenleving waar het relatief eenvoudig is afwijkende ideeën en ideologieën te ontwikkelen. Alhoewel er hier en daar een deukje in ons internationale imago komt, staan we toch nog steeds bekend als tolerant en open voor afwijkende ideeën. Tegelijkertijd is het te eenvoudig om onze inspanningen rond veiligheid alleen te richten op gevaar van buitenaf. Niet voor niets

wordt veiligheid steeds nadrukkelijker gekoppeld aan welbevinden en welzijn. Nog niet zo lang geleden werden een muur met prikkeldraad, wapens en een mijnenveld gezien als belangrijkste verdediging tegen het kwaad, dat toen nog gewoon uit het oosten leek te komen. De opvattingen over veiligheid zijn radicaal verschoven: van fysiek beveiligen tegen mogelijk gevaar door een bekende (zichtbare) vijand, naar het intrinsiek veilig maken van een omgeving waar de 'kwaadwillenden' niet meer als zodanig herkenbaar zijn. En waarbij de methoden en technieken nog maar ten dele tastbaar zijn. De aanslagen van 11 september 2001 hebben een verandering gebracht in ons denken over veiligheid. De veronderstelde dreiging van meer aanslagen en de schade voor de wereldeconomie dreunt anno 2010 nog steeds door en gaat veel verder dan de aanslagen op zich. Naast de nadruk op informatievoorziening en informatie delen (zie het hoofdstuk 'De grens voorbij') is er nu meer aandacht voor intrinsieke veiligheid. In onze eigen Tweede Kamer liep al vóór de aanslagen een discussie over veiligheid in het algemeen en ICT in het veiligheidsdomein in het bijzonder. Vlak na de aanslagen verschoof de aandacht en werd het beleid meer gericht op het beveiligen en in stand houden van vitale infrastructuren. Vitale infrastructuren zijn de voorzieningen die Nederland nodig heeft voor welvaart en welzijn van onze maatschappij (burgers en organisaties). U leest er meer over in het hoofdstuk 'Vitale infrastructuren op weg naar volwassenheid'.

Ook niet-vitale organisaties worden zich meer bewust van hun kwetsbaarheid. Daar waar voorheen vooral aandacht werd besteed aan safety in de vorm van patiëntveiligheid, arbo- en milieuvraagstukken, groeit de aandacht voor security. Hoe kan een organisatie haar weerbaarheid tegen moedwillige inbreuken op veiligheid verhogen? Welke waarden binnen de organisatie zijn belangrijk en welke risico's worden daarmee gelopen? Integrale veiligheid, waarover u leest in het hoofdstuk 'Beheerst u integrale veiligheid in uw organisatie?' kan bijdragen aan belangrijke verbeteringen op dit punt.

We staan ook stil bij de burger. Hoe ervaart hij het begrip veiligheid en hoe ziet hij zijn eigen rol daarin? Door de toegenomen aandacht voor (bijna) incidenten lijken we angstiger dan vroeger. De paniek die een verwarde man bij de dodenherdenking op de Dam kon veroorzaken, is daartoe illustratief. Desondanks vraagt de overheid steeds vaker aan de burger om alert te zijn en mee te kijken omwille van betere veiligheid en effectievere misdaadbestrijding. Vanuit het perspectief van beperkte capaciteit is dat begrijpelijk, maar wat vindt de burger daar eigenlijk van? We belichten drie soorten reacties in het hoofdstuk 'Veiligheid, wat moet ik ermee?'

De burger staat ook centraal waar het gaat om kwaliteit van de hulpverleningsdiensten. Politie, Geneeskundige Hulpverlening bij Ongevallen en Rampen (GHOR) en brandweer proberen continu de kwaliteit van hun processen en diensten te verbeteren ten behoeve van de (soms onwillige) klant: de burger. De brandweer heeft daarbij geconstateerd dat een radicale verandering nodig is om zichzelf verder te kunnen ontwikkelen. Ondanks verdubbeling van de kosten is het resultaat in termen van aantallen doden en gewonden als gevolg van incidenten gelijk gebleven. In het hoofdstuk 'Kwaliteitsslag bij de brandweer: waar is de brand?' wordt gewaarschuwd voor formalisering, regulering en normering als instrumenten om kwaliteit te verbeteren. De sleutel tot kwaliteitsverbetering ligt in het hart van de organisatie, bij de onderliggende principes van de individuele brandweerman/vrouw.

Veiligheid is een issue, overal. We kunnen er niet omheen. U ook niet. Vandaar deze eerste editie van Trends in Veiligheid. Om met u en uw organisatie in gesprek te gaan over uw kijk op de ontwikkelingen in het veiligheidsdomein. En om u te inspireren tot nieuwe ideeën of concrete maatregelen in uw eigen organisatie. Wacht niet te lang, want dit issue komt op uw pad. Vroeg of laat.

Drs. Erik Hoorweg MCM is managementconsultant bij Capgemini en richt zich op besturing en beheersingsvraagstukken, organisatiedoorlichting en intelligence binnen het veiligheidsdomein. Drs. Nico Kaptein is als principal consultant bij Capgemini werkzaam als vakgroepleider Public Security en director of Operations Public Security binnen de global Public Sector.

1 De bestuurlijke aanpak van georganiseerde misdaad in Nederland

Een beschouwing op een alternatieve bestrijding van de georganiseerde misdaad.

Drs. Abderrahman Kaouass
Drs. Tjarda Hersman
Drs. Erik Staffeleu

"Ook in de hennepteelt zien we steeds meer verwevenheid tussen onder- en bovenwereld. Er zijn veel mensen schatrijk geworden met hennep. In tien jaar ben je miljonair. Veel van dat geld wordt geïnvesteerd in de bovenwereld, in vastgoed. Het begint met een pandje, dat je goedkoop opknapt en er een hennepplantage inzet. Na een paar oogsten verkoop je het pand en houd je 30.000, 40.000 euro winst over - wit geld. Op een gegeven moment is het interessanter gewoon pandjes te kopen, in plaats van er hennep in te pompen. Het zijn mensen die nu veel geld geven aan Unicef en Ronald McDonald en die de lokale tennisvereniging sponsoren."
(Interview Max Daniel, politiekorps Friesland in NRC Handelsblad op 18 oktober 2008)

Noodzaak bestuurlijke aanpak

De georganiseerde misdaad in Nederland is een bloeiende bedrijfstak waar jaarlijks vele miljarden euro's in omgaan. De gevolgen hiervan hebben een behoorlijke impact op de samenleving. Het gaat om aantasting van de openbare orde, teloorgang en verpaupering van straten en wijken, grootschalige criminele investeringen in vastgoed en de groeiende vervlechting tussen de onder- en bovenwereld. Het meest duidelijke voorbeeld van de verwevenheid tussen onder- en bovenwereld is de vastgoedfraude.
Personen uit respectabele beroepsgroepen zoals notarissen en advocaten lijken vaak op dubieuze wijze betrokken te zijn bij witwasconstructies. Dat roept vele vragen en onzekerheden op en leidt uiteindelijk tot de aantasting van het maatschappelijk bestel en de legitimiteit van de overheid. Om de vervlechting tussen de onder- en bovenwereld beter aan te pakken, richt de overheid zich sinds eind jaren negentig op de bestuurlijke aanpak van georganiseerde misdaad. Dit als antwoord op het falen van het strafrecht als enig strafmiddel. Het doel van dit hoofdstuk is om in te gaan op het verschijnsel 'bestuurlijke aanpak georganiseerde misdaad'. Wat is de (politieke) aanleiding geweest? Waarin uit zich de verwevenheid tussen onder- en bovenwereld? Welke verschijningsvormen van bestuurlijke aanpak bestaan er? En, welke toekomstontwikkelingen voorzien wij op dit gebied?

Politieke context van de bestuurlijke aanpak

De verwevenheid tussen onder- en bovenwereld kreeg voor het eerst politieke en maatschappelijke aandacht door de parlementaire enquêtecommissie Opsporingsmethoden (Commissie Van Traa). Deze parlementaire enquêtecommissie constateerde op drie vlakken een crisis in de opsporing van georganiseerde misdaad: een gezagscrisis (ontbrekende normen), een legitimiteitscrisis (problemen in de gezagsverhoudingen) en een organisatiecrisis (een niet goed functionerende opsporingsorganisatie). Deze crisis in de opsporing maakte het dat de puur strafrechtelijke aanpak van georganiseerde misdaad niet afdoende was. Criminele groeperingen moesten vroegtijdig opgespoord en geraakt worden, daar waar ze het gevoeligst zijn: via witwassen en het investeren van misdaadgelden (bijvoorbeeld het kopen van panden). Het blijkt immers dat de georganiseerde misdaad de bovenwereld op verschillende manieren nodig heeft. Dat is niet alleen voor het via illegale activiteiten verdienen aan legale sectoren, maar ook voor het investeren en witwassen van misdaadgeld. De parlementaire enquête van de

Commissie Van Traa is vervolgens een belangrijke stimulans geweest voor de verdere aanpak van de georganiseerde misdaad. Zowel de strafrechtelijke als de bestuurlijk-preventieve aanpak kregen een impuls.

Na het rapport van de Commissie Van Traa zijn er verschillende landelijke en lokale initiatieven ontstaan om de georganiseerde misdaad bestuurlijk aan te pakken. Op landelijk niveau is het Programma bestuurlijke aanpak georganiseerde misdaad in het leven geroepen en op het gebied van wetgeving de Wet BIBOB.[1] Als een ondernemer een vergunning aanvraagt, moet hij conform de BIBOB-wet inzage geven in onder meer zijn financiële administratie, de eigendomsverhoudingen binnen zijn bedrijf, de herkomst van zijn geld en zijn personeelsbeleid. Als uit die informatie het vermoeden rijst dat er mogelijk sprake is van criminele activiteiten, kan de betrokken overheidsinstantie, bijvoorbeeld een gemeente of een provincie, besluiten om de vergunning niet te verlenen of een bestaande vergunning in te trekken. Alvorens we nader ingaan op het verschijnsel bestuurlijke aanpak, geven wij eerst enkele feiten weer over georganiseerde misdaad en de verwevenheid van onder- en bovenwereld.

Feiten over verwevenheid onder- en bovenwereld

Het uitgangspunt van de bestuurlijke aanpak is dat de overheid crimineel gedrag niet dient te faciliteren. Impliciet wordt hiermee verondersteld dat de overheid voldoende mogelijkheden heeft om te voorkomen dat criminelen misbruik maken van bepaalde publieke voorzieningen. De aard van de Nederlandse georganiseerde misdaad verschilt met bijvoorbeeld die van Italië of New York, waar deze zich uit in het op illegale wijze controleren van legale markten, zoals handelen in gestolen auto's. De georganiseerde misdaad in Nederland manifesteert zich echter vooral op illegale markten, zoals smokkel van drugs en illegalen. De aard van de Nederlandse georganiseerde misdaad compliceert de bestuurlijke aanpak. Illegale markten zijn niet door de overheid gereguleerd met als gevolg dat er met minder bestuurlijke instrumenten opgetreden kan worden. De bestuurlijke instrumenten komen namelijk pas in beeld wanneer gebruik wordt gemaakt van legale voorzieningen, zoals vergunningen voor huisvesting.[2]

Het onderscheid tussen georganiseerde misdaad en organisatiecriminaliteit is hierbij van belang. Bij georganiseerde misdaad gaat het om het illegale handelen van criminele groeperingen die als primair oogmerk hebben criminele winst te behalen door middel van illegale handelingen. De georganiseerde misdaad in Nederland bestaat voor het overgrote deel uit handel in drugs. Andere illegale markten, zoals wapenhandel komen zeker voor en vormen op zichzelf een ernstig probleem, maar de omvang en omzet zijn veel geringer. Bij de drugscriminaliteit gaat het om illegaal geld en geweld als functie van de illegale markt. De investeringen van crimineel verdiend geld worden gedaan rond de illegale markten in de horeca of het onroerend goed. De grootste bedreigingen gaan uit van de macht van witgewassen en illegaal geld, het gebruik van afpersing en geweld, en de pogingen tot corruptie van de overheid.

Organisatiecriminaliteit houdt in het illegale handelen van op zichzelf legale organisaties, die als primair oogmerk hebben zich als legale organisatie te handhaven met behulp van illegale handelingen. Bekend is dat organisatiecriminaliteit voorkomt in bijvoorbeeld de afvalverwerkingsindustrie en prostitutie. De signalen die een gemeente opvangt van georganiseerde misdaad en organisatiecriminaliteit zijn uitbuiting van specifieke groepen inwoners of rechtspersonen door criminelen; criminelen die zich onroerend goed verwerven en/of bedrijvigheid ontplooien, en onroerend goed waarin criminele activiteiten ontplooid worden. Dit heeft negatieve effecten op een gemeente. Niet alleen de rechtsorde is aangetast, maar ook de veiligheid en leefbaarheid van groepen inwoners en ondernemers is aangetast door de verloederende werking die met de aanwezigheid van criminaliteit gepaard gaat. Red light districts bijvoorbeeld ervaren weinig zorg voor de openbare ruimte, overlastgevende clientèle en geluidsoverlast. Voorts is hiermee de integriteit van de economische sector en het lokaal bestuur aangetast. Ondernemers die tegen criminele collega-ondernemers moeten opboksen zijn benadeeld. Het ontduiken van regelgeving betekent voor de gemeente een afnemende werkingskracht van beleid. In het ergste geval ontstaat er een soort no-gozone, waar

[1] BIBOB staat voor Wet bevordering integriteitsbeoordelingen door het openbaar bestuur. Overheden (zoals gemeenten) kunnen de achtergrond van een bedrijf of persoon onderzoeken bij een af te geven of afgegeven vergunning of subsidie of bij het gunnen van een overheidsopdracht.
[2] Zie o.a. W. Huisman, M. Huikeshoven, H. Nelen, H. van de Bunt en J. Struiksma, 'Het Van Traa-project. Evaluatie van de bestuurlijke aanpak van georganiseerde criminaliteit in Amsterdam', Boom Juridische uitgevers, Den Haag 2005

criminelen relatief ongehinderd hun activiteiten ontplooien met als gevolg dat de gemeente geen greep en zicht heeft op wat er zich voltrekt.[3]

Er zijn geen exacte cijfers over de omvang van de georganiseerde misdaad en de verwevenheid van onder- en bovenwereld. De *omvang* hiervan laat zich niet verantwoord in harde cijfers uitdrukken - noch naar omzet noch naar aantallen groepen. Daarvoor is het beeld te gedifferentieerd. Echter, deskundigen zijn wel van mening dat het eerder om een paar miljard euro's gaat dan om miljoenen euro's.
De verwevenheid van de onder- en bovenwereld bemoeilijkt de handhaving. Uit meerdere onderzoeken blijkt dat bijvoorbeeld bij het misbruik van vastgoed tussen de criminele onderwereld en de nette bovenwereld geen eenvoudige scheiding is aan te brengen. Wel blijkt echter dat criminelen de hulp van zakelijke dienstverleners nodig hebben om 'foute' vastgoedtransacties uit te kunnen voeren. In strafrechtelijke dossiers komen regelmatig financiële ondernemingen, makelaars, taxateurs, notarissen, belastingadviseurs, trustkantoren, advocaten en accountants naar voren (ministerie van Justitie, 2008). Waar kan de bestuurlijke aanpak hier de strafrechtelijke aanpak ondersteunen?

Verschijningsvormen van de bestuurlijke aanpak

De beoogde versterking op het terrein van de preventieve en bestuurlijke aanpak van georganiseerde misdaad richt zich enerzijds op het versterken van de *samenwerking* tussen veiligheidspartners om te komen tot een *geïntegreerde aanpak* (bestuurlijk, strafrechtelijk en fiscaal) en anderzijds op het versterken van het gebruik van het bestuursrechtelijk instrumentarium.

Samenwerking - geografische focus vs. thematische focus

Aan samenwerkingsinitiatieven die erop gericht zijn de informatiepositie ten aanzien van georganiseerde misdaad te versterken en de aanpak op elkaar af te stemmen is geen gebrek. De samenwerkingsinitiatieven blijken echter nog niet altijd even succesvol. Hierbij is het goed een onderscheid te maken naar samenwerkingsinitiatieven met een thematische dan wel een geografische focus. Het meest opvallende initiatief met een thematische focus van de recente jaren is de inrichting van thematische expertisecentra, zoals het Expertisecentrum Mensenhandel/Mensensmokkel (EMM), het Financieel Expertise Centrum (FEC) en het Vastgoed Intelligence Center (VIC).

Het meest opvallende initiatief met een regionale focus is de oprichting van elf Regionale Informatie en Expertise Centra (RIEC's). Het RIEC is in het leven geroepen om als informatieknooppunt en expertisecentrum op te treden ten aanzien van de bestuurlijke aanpak van georganiseerde misdaad. Een RIEC kent de volgende deeltaken:

- uitwisselen van informatie (op basis van een convenant);
- inbrengen van expertise en kennis in diverse bestuurlijke processen (vergroten van kennis en capaciteit);
- ondersteunen van provincies en gemeenten bij het tegenhouden van

Het Expertisecentrum Mensenhandel/Mensensmokkel

- Het Expertisecentrum Mensenhandel/Mensensmokkel is een samenwerkingsverband tussen de politie, de Immigratie- en Naturalisatiedienst, Koninklijke Marechaussee en de Sociale Inlichtingen- en Opsporingsdienst. Bij het EMM komen onder andere signalen van mensenhandel en mensensmokkel van deze verschillende organisaties bij elkaar.
- Het Financieel Expertise Centrum is een multidisciplinair samenwerkingsverband van zeven organisaties met een toezicht-, controle-, opsporings- en vervolgingstaak in de financiële sector.
- Het Vastgoed Intelligence Center is een landelijk opererend samenwerkingsverband waarbinnen het Openbaar Ministerie, de Belastingdienst, de FIOD-ECD, de FIU en de politie een platform hebben ingericht voor informatie-uitwisseling en -analyse van vastgoedgerelateerde, georganiseerde misdaad.

[3] Zie o.a. SGBO, Onderzoeks- en adviesbureau van de VNG, 'Bestuurlijke aanpak van georganiseerde criminaliteit: ongewoon gewoon. Een handreiking voor gemeenten.' VNG uitgeverij, Den Haag, 2002.

RIEC's geografische focus

1. Noord
2. Oost-Nederland
3. Midden-Nederland
4. Noord-Holland
5. Haaglanden/Hollands-Midden
6. Zuid-Holland-Zuid
7. Zeeland, Brabant-Noord, Midden- en West-Brabant
8. Limburg
9. Zuidoost-Brabant
10. Rotterdam/Rijnmond
11. Gelderland Midden-Zuid

verwevenheid van onder- en bovenwereld (Wet BIBOB) en handhaven (bestuurlijke tools).

De RIEC's vormen een samenwerkingsverband voor alle aangesloten provincies, gemeenten, OM, politie, de bijzondere opsporingsdiensten, de belastingdienst en andere (semi)overheden. Door informatie van de verschillende partijen regionaal te bundelen en te analyseren beogen de RIEC's een goed beeld te ontwikkelen van criminele organisaties en activiteiten in de gehele regio. RIEC's ondersteunen de samenwerking tussen strafrechtelijke en bestuurlijke partijen. Zij vormen als het ware een shared services organisatie voor de capaciteit en expertise van bestuurlijke maatregelen. De samenwerking dient te leiden tot een intensievere informatie-uitwisseling tussen alle samenwerkende partners en een beter gebruik van de bestuurlijke mogelijkheden in de aanpak van georganiseerde misdaad. Ten slotte streven de RIEC's ernaar om de onderlinge afstemming van strafrechtelijk en bestuurlijk handhavend optreden op regionaal niveau te ondersteunen. De RIEC's kennen primair een geografische focus waarbij thematische prioriteiten gesteld worden (onder andere mensenhandel, vastgoed en hennepteelt).

Het samenbrengen van de veiligheidspartners rondom een thema blijkt niet ingewikkeld. Het is echter niet altijd even eenvoudig om vervolgens ook de benodigde informatie te delen (op strategisch, tactisch en operationeel niveau) en daadwerkelijk geïntegreerd op te treden. Het is vooral de diversiteit aan obstakels die hiervoor zorgt, niet zozeer de omvang van de obstakels. Zo worden de landelijke wettelijke kaders waaronder informatiedeling mogelijk is, steeds duidelijker en worden er technische maatregelen getroffen om meer informatie-uitwisseling mogelijk te maken. Het inzicht in ieders informatiepositie en de wil om bij te dragen aan het gezamenlijk belang zonder dat het in het eigen belang is, vormen echter een uitdaging.

Instrumenten voor de bestuurlijke aanpak

Vanuit de samenwerkingsinitiatieven volgen adviezen aan de veiligheidspartners om de strafrechtelijke, fiscale en bestuurlijke aanpak vorm te geven. Er zijn veel instrumenten die ingezet kunnen worden om de bestuurlijke aanpak vorm te geven. Met de versterking van de bestuurlijke aanpak wordt beoogd gerichter gebruik te maken van de wettelijke instrumenten om zo de effectiviteit te vergroten. Het instrument dat momenteel de meeste aandacht krijgt is de Wet BIBOB, een bewezen instrument om informatie te verkrijgen ter voorkoming van het onbedoeld faciliteren van criminaliteit door de lokale overheid. De Wet BIBOB geeft gemeenten de bevoegdheid om vergunningen en subsidies te weigeren of in te trekken. De RIEC's dienen het gebruik van de Wet BIBOB effectiever en efficiënter te maken en hiertoe de juiste ondersteuning aan lokale overheden te bieden.

Naast de Wet BIBOB geeft vooral de Algemene wet bestuursrecht (Awb) gemeenten een uitgebreid instrumentarium om handhavend op te treden. Tevens heeft de gemeente mogelijkheden om panden te sluiten of zelfs te onteigenen op basis van diverse overige wetten (onder andere Gemeentewet). Het richten van speciaal lokaal beleid op het tegengaan van bepaalde vormen van georganiseerde misdaad,

evenals het aanpassen van het beleid ten aanzien van verordeningen en vergunningen, kan eveneens ingezet worden als bestuurlijk instrument tegen georganiseerde misdaad.

Hierbij kan gedacht worden aan specifieke Algemene Plaatselijke Verordeningen (APV's) en het aanpassen van bestemmingsplannen. Gemeenten hebben een uitgebreid instrumentarium. Om hiervan gericht gebruik te maken zal men zich bewust moeten zijn van het nut en de noodzaak om de bestuurlijke aanpak te professionaliseren en de instrumenten gerichter in te zetten.

Van versnippering naar focus

De veelheid aan samenwerkingsinitiatieven, die een thematische dan wel geografische insteek hebben, gecombineerd met de veelheid van wettelijke instrumenten die ingezet kunnen worden voor de bestuurlijke aanpak, betekenen dat de toekomst van de bestuurlijke aanpak van georganiseerde misdaad ligt in het maken van keuzes en het aanbrengen van focus. Dit betekent het aanbrengen van een gerichte focus op samenwerking, een duidelijke prioriteitsstelling in thema's en een heldere keuze in de aanpak.

Het samenbrengen van thematische samenwerkingsinitiatieven op landelijk niveau in thematische expertisecentra moet de obstakels in het daadwerkelijk uitwisselen van informatie en het geïntegreerd optreden gaan beslechten. De RIEC's kunnen de randvoorwaarden voor informatie-uitwisseling en geïntegreerd optreden van veiligheidspartners realiseren en de effectiviteit van de bestuurlijke instrumenten inzichtelijk maken. De doelstelling zou moeten zijn om veel van de geografische samenwerkingsinitiatieven, gericht op de bestuurlijke aanpak van georganiseerde misdaad samen te brengen onder de vlag van het RIEC.

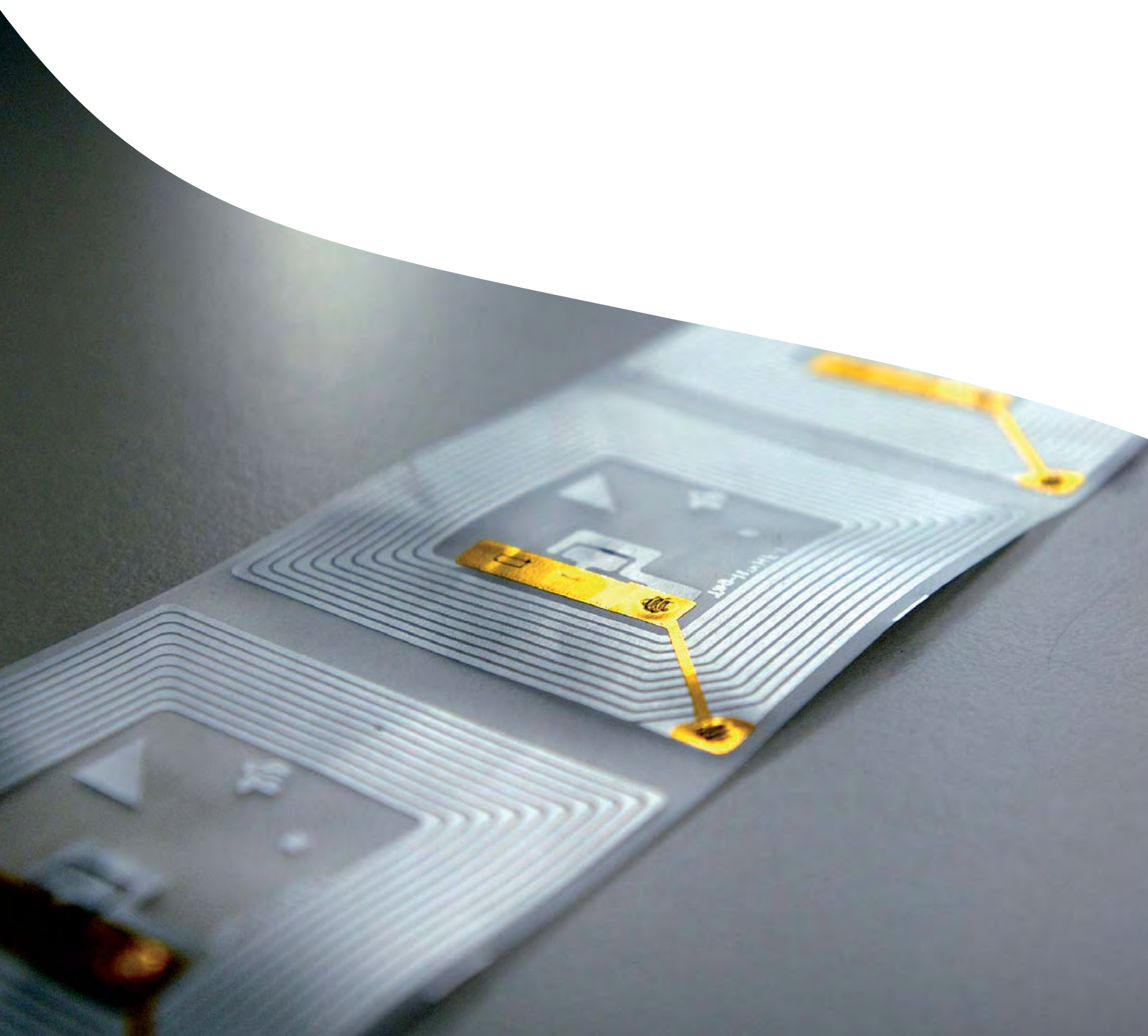
Dit brengt de RIEC's meer in positie om de regierol in de bestuurlijke aanpak op te pakken op (boven)regionaal niveau. Om daarbij optimaal gebruik te maken van de landelijke thematische expertisecentra is het wenselijk dat de regionale prioriteiten van de RIEC's aansluiten bij de thema's van de expertisecentra (vastgoedfraude, mensenhandel en -smokkel en financiële criminaliteit).

De thematische prioriteiten van het RIEC worden vastgesteld door de regionale stuurgroep, of de lokale driehoeken (gemeente-politie-OM). Te vaak worden er te veel prioriteiten gesteld. Er komen wel steeds nieuwe prioriteiten bij in de aanpak van georganiseerde misdaad, maar er gaan geen prioriteiten af. Doelstelling moet zijn om periodiek een beperkt aantal thematische prioriteiten te stellen, afgeleid van landelijk geprioriteerde thema's. Tenslotte moet het doel zijn om meer professionaliteit te realiseren in het gebruik van het bestuurlijk instrumentarium voor de aanpak van georganiseerde misdaad. Dit betekent dat er inzicht moet komen in de effectiviteit van de verschillende instrumenten en dat geïnvesteerd moet worden in het verhogen van de kwaliteit van het gebruik van die instrumenten, waarmee het meeste resultaat kan worden bereikt. De expertisecentra en de RIEC's kunnen hierin een essentiële rol vervullen.

Tot slot

In dit hoofdstuk is het verschijnsel bestuurlijke aanpak van georganiseerde misdaad als relatief nieuw fenomeen in de overheidsaanpak beschreven. De bestuurlijke aanpak van georganiseerde misdaad zal in de toekomst een steeds belangrijkere rol krijgen. Het gaat immers om het bestrijden van de voedingsbodem van georganiseerde misdaad. De bestrijding van de georganiseerde misdaad dient niet alleen door politie en justitie plaats te vinden. Een betere samenwerking tussen de veiligheidspartners, het beter en sneller kunnen delen van informatie en een uniform nationaal beleid zijn hierbij de kernbegrippen.

Drs. Abderrahman Kaouass, drs. Tjarda Hersman en drs. Erik Staffeleu zijn managementconsultants bij Capgemini. Abderrahman Kaouass is gespecialiseerd in bestuurlijke veiligheidsvraagstukken. Tjarda Hersman is bestuurskundige en criminoloog en nauw betrokken bij nationale veiligheidsvraagstukken.
Erik Staffeleu is gespecialiseerd in intelligencevraagstukken en intelligence gestuurd optreden.



2 Ter land, ter zee, in de lucht en op het web

Naar een integrale strategie voor digitale defensie.

Mike Tettero
Mr. Patrick de Graaf

Conflicten worden in deze tijd ook op het digitale slagveld uitgevochten. Nederland heeft een integrale militaire cyberstrategie nodig. In dit hoofdstuk geven wij hiervan een 'sneak preview'.

De digitale dreiging is reëel

Bedreigingen voor Westerse samenlevingen komen steeds vaker ook uit cyberspace. In 2007 zetten Russische hackers met een Denial of Service (DoS) Estse websites van de financiële wereld, de media en de overheid op zwart. Dit als vergelding op het weghalen van een Russisch standbeeld in Estland. In hetzelfde jaar legde een aanval van Chinese hackers een deel van het Pentagon-netwerk plat. Vlak voorafgaand aan de Russische inval in Georgië in 2008 werden vele websites van Georgië onbereikbaar en werd de president op zijn eigen site afgebeeld als nazi. De (unclassified) mailbox van de minister van Defensie van de Verenigde Staten werd gekraakt in 2007. Onder cyber warfare valt ook een (niet officieel bevestigde) sabotage van een Sovjet-pijpleiding in 1982 door het in omloop brengen van opzettelijk foutief functionerende computerchips en programmatuur.[1] De daaropvolgende drie kiloton zware ontploffing van de pijpleiding was tot in de ruimte te zien… Westerse landen ondervinden elk jaar tienduizenden kleine en minder kleine cyberaanvallen, met name gericht op het verzamelen van inlichtingen over het militaire apparaat, energievoorziening, luchtverkeersleiding en financiële markten.

Ook Nederland is kwetsbaar voor cyberaanvallen, gezien onze open economie en hoogwaardige communicatievoorzieningen, zichtbaarheid in de internationale samenleving en een hoge afhankelijkheid van ICT voor het reilen en zeilen van de samenleving. Uitval of verstoring van of verlies aan vertrouwen in digitale voorzieningen is desastreus voor onze economie en samenleving als geheel. Eind 2009 verschenen er berichten in de pers[2] over het ontbreken van een cyberstrategie bij het ministerie van Defensie. Nederland heeft gezien de externe bedreigingen een cyberstrategie en een cyberleger nodig, in navolging

Er is geen consensus over de definities van cyberspace en cyber warfare of defence. Wij gaan hier uit van de volgende beschrijvingen

- Cyberspace: het World Wide Web, maar ook andere vormen van digitale activiteiten in netwerken met anderen. De digitale communicatie van elektronische regel- en meetsystemen van bijvoorbeeld energievoorziening of chemische installaties valt er ook onder en eveneens de hardware en software waaruit die systemen bestaan.
- Cyber warfare of cyber defence: conflictbeslechting in cyberspace met middelen als hacken en afluisteren van informatiestromen, saboteren van elektronische systemen en uitschakelen van vijandige websites, dan wel de bescherming tegen dergelijke aanvallen. Cyber warfare en cyber defence worden beide hiervoor in de praktijk gebruikt. We hanteren verder de term cyber defence.

[1] Voorbeeld aangehaald in W.K. Clark, P.L. Levin, 'Securing the information highway: how to enhance the United States' Electronic Defenses', Foreign Affairs, november 2009.
[2] Zie bijvoorbeeld een artikel in De Pers (http://depersnew.republisher.modernmedia.nl/238726/De_Pers_dinsdag_10_november_2009.pdf).

Verschillende vormen oplopend in het geweldsspectrum

Soort cyber attack	Cyber-vandalisme	Misdaad via internet	Cyber crime	Cyber-terrorisme	Cyber warfare/ defence
Actor	Potentieel iedereen op internet	Criminelen	Criminelen	Politieke/ ideologische groeperingen	Nationale staten
Doelwit (domein)	Digitaal	Fysiek	Digitaal	Fysiek	Fysiek en digitaal
Motief	Genot, afreageren	Gewin, genot	Gewin	Ideologisch, politiek	Politiek
Schade	Beperkt en gericht	Wisselend, kan aanzienlijk zijn	Wisselend, kan aanzienlijk zijn	Doorgaans gericht	Gericht tot omvangrijk
Benodigde organisatie-graad daders	Laag	Laag-middel	Laag-middel	Laag-middel	Middel-hoog
Voorbeelden	Defacing van websites, beledigende tweets of comments	Kinderporno, stalking, piraterij, racisme	Phishing, Denial of Service, digitale inbraak, industriële spionage	Sabotage vitale voorzieningen	Spionage, sabotage vitale voorzieningen, censuur via DoS.
Primaire actoren bestrijding	Providers, webmasters	Politie, OM	Politie, OM, eigen bescherming	NCTb, AIVD, MIVD, eigen bescherming	Defensie

van landen als de Verenigde Staten, Groot-Brittannië, China, Duitsland en Rusland en vermoedelijk ook Iran en Noord-Korea.
De uitbreiding van de strategie van Defensie met een cybercomponent is primair een politiek onderwerp. De politiek bepaalt immers het speelveld van de krijgsmacht. De Tweede Kamer heeft de minister van Defensie verzocht aan te geven wat de aanpak voor digitale verdediging is. De minister heeft daarop in maart 2010 bij brief aan de Tweede Kamer aangegeven welke maatregelen hij momenteel heeft genomen.[3] Deze passeren later in dit stuk de revue. Een (integrale) beleidsvisie is bij schrijven nog in ontwerp. We bieden hier een 'sneak preview' van wat zo'n cyberstrategie zou kunnen inhouden.

Cyber wat?

In de praktijk worden veel termen voor kwaadaardig gedrag in cyber space door elkaar gebruikt en met wisselende definities: cyber warfare, cyberterrorisme, cyber defence, cyber crime, hacktivisme etc. Achter deze termen gaan verschillende verschijnselen schuil, die met elkaar gemeen hebben dat ze internet en andere digitale wegen gebruiken om eigen (politieke) belangen te dienen en die van anderen te schaden. Doelwit, actor, motief, organisatiegraad en potentiële schade verschillen echter aanzienlijk, wat cruciaal is voor de wijze van bestrijding en wie daarvoor de eerst aangewezen verantwoordelijke is.

Cyber defence, gericht op fysieke en omvangrijke financiële schade beschouwen we als de zwaarste in het digitale geweldsspectrum. Bij dergelijke cyber

[3] Kamerstuk 2009-2010, 26643, nr. 149, Tweede Kamer.

attacks gaat het om (militaire) spionage, zoeken naar zwakke plekken, vingeroefeningen voor echte aanvallen, kleinschalige schermutselingen in cyberspace of de ondersteuning van daadwerkelijke fysieke conflicten.

Internationaal brengen naties hun digitale defensie op orde

Sinds eind jaren negentig zijn militaire grootmachten als de Verenigde Staten begonnen met het beschrijven van het fundament van cyber defence. De Verenigde Staten publiceerden in 1998 hun Joint Publication 3-13 over Information Operations. Deze doctrine zet cyber defence in een breder perspectief van niet-fysieke oorlogsvoering. Datzelfde deden Qiao Liang en Wang Xiangsui, beiden kolonels in het Chinese leger, in hun strategie 'Unrestricted Warfare'.[4] Hierin beschrijven zij hoe een land als China een technologisch superieur land als de Verenigde Staten met een combinatie van middelen kan verslaan. Opvallend aan dit document is dat geen enkel domein (economisch, crimineel, informatie, psychologisch en dergelijke) als strijdtoneel wordt uitgesloten.
Deze en andere landen - bijvoorbeeld Duitsland en Groot-Brittannië - ontwikkelen nu hun integrale cyberveiligheidsstrategieën en operationele vaardigheden voor cyber defence. Het Pentagon installeerde in 2009 als voorlopig hoogtepunt een volwaardig Cyber Command (USCYBERCOM), te leiden door een viersterrengeneraal of een viceadmiraal.[5] In hetzelfde jaar stelde president Obama ook een Cyber Security Chief aan, met als opdracht het formuleren en (doen) uitvoeren van een integrale (civiele) cyberstrategie voor de Verenigde Staten. De diverse recente berichten over de aanval op Google en gecompromitteerde USB-sticks voor Britse diplomaten laten zien dat ook China zijn cyberoperaties serieus neemt en daadwerkelijk inzet. Niet alleen naties, ook georganiseerde groepen gebruiken het digitale wapen voor psychologische of fysieke oorlogsvoering. Het digitale wapen is namelijk erg aantrekkelijk. Het is goedkoop, snel, anoniem en het gebruik kent lage risico's voor de dader. De schade is echter groot en precies toe te brengen. Soms acteren dergelijke groepen in het verlengde van een landsbelang, soms ook uit eigen ideologische motivatie, aanzien bij de eigen groep of financieel gewin.

De NAVO heeft na de digitale aanval op Estland het onderwerp cyber defence drie concrete initiatieven genomen:

1. Op operationeel niveau de vorming van een nieuwe Cyber Defence Management Authority (CMDA, Brussel), om operationele cyber defence-activiteiten van alle lidstaten te bundelen. De CMDA zal naar verwachting uitgroeien tot een warroom voor de cyber defence van de NAVO, waarbij de daadwerkelijke tactische respons op aanvallen wordt uitgevoerd door lidstaten (in een coalition of the willing).
2. Oprichting van het Cooperative Cyber Defence (CCD) Centre of Excellence (CoE), gevestigd in Tallinn, Estland. Dit Centre of Excellence heeft als doel de vorming van doctrine en strategie te bevorderen ten aanzien van cyber defence. Nederland is hiervan vooralsnog geen actief sponsorland.
3. Versneld versterken van de beveiliging van de eigen netwerken.

Zowel operationeel als intellectueel neemt de NAVO dus de handschoen van het digitale slagveld op.

Nederland moet een achterstand inhalen

Vanuit de Nationale Veiligheidsstrategie zijn belangrijke publieke en publiek-private initiatieven tot stand gebracht ter bescherming van de vitale infrastructuur van Nederland. Denkt u aan GOVCERT[6] en het publiek-private Nationale Infrastructuur Cyber Crime (NICC).[7] De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) waarschuwen ons verder voor digitale spionage.[8] Het ministerie van Defensie zit ook niet stil, neemt deel aan GOVCERT en heeft DEFCERT (Defensiebreed Computer Emergency Response Team) opgericht. DEFCERT richt zich op adviesverstrekking over beveiliging van Defensie IT-systemen en neemt maatregelen bij incidenten. Ook wordt er een hoogwaardig Intrusion Detection System ontwikkeld.

[4] http://www.c4i.org/unrestricted.pdf. Zie ook: http://defensetech.org/2009/03/03/confronting-unrestricted-warfare/
[5] http://online.wsj.com/public/resources/documents/OSD05914.pdf.
[6] GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid. GOVCERT verricht activiteiten op het gebied van preventie, signalering, kennisdeling, monitoring en begeleiding bij incidenten. Veel overheden zijn deelnemer van GOVCERT. Zie verder www.govcert.nl.
[7] Het doel van het programma NICC is één publiekprivate, geïntegreerde aanpak van veilig digitaal werken, ofwel één sluitende Nationale Infrastructuur ter bestrijding van Cybercrime. Zie www.samentegencybercrime.nl.
[8] https://www.aivd.nl/@125345/drie-publicaties#616871.

Wat zou een militaire cyberstrategie moeten bevatten?

- De nationale doelstelling ten aanzien van het gebruik en veiligheid van cyberspace. De doelstelling zou in elk geval moeten onderstrepen dat de digitale infrastructuur een essentieel onderdeel is van de Nederlandse vitale infrastructuur. Nederland verklaart zich bereid om die infrastructuur met defensieve en offensieve middelen te verdedigen uit landsbelang.
- De rol die Nederland voor zichzelf ziet in cyberconflicten en de wijze van optreden, aansluitend op het geschetste ambitieniveau. Welk soort middelen zetten we in en waar in het geweldsspectrum? Wat ons betreft beperken die middelen zich niet tot het beschermende 'harnas', maar is het inclusief het 'zwaard' voor een proactieve verdediging.
- De wijze waarop onze militaire cybercapaciteiten zijn georganiseerd en hoe dit moet worden gerealiseerd met mensen, middelen en financiën.
- De zienswijze op de nationale en internationale samenwerking, zowel publiek als privaat: bijvoorbeeld NICC, NAVO's CMDA voor de operatie en de CCD CoE voor strategie en juridica. Intensieve samenwerking en wederzijdse ondersteuning met de andere 'cyber warriors' in het publiek-private speelveld zijn onmisbaar, al is het maar om kennisuitwisseling en het verkrijgen van een digitale 'situational awareness'.
- De definiëring en uitwerking van het juridisch kader. Belangrijke vragen die hier spelen zijn bijvoorbeeld de afbakening van het digitale gebied waarop Nederland mag opereren (stel dat programmatuur van een Nederlandse organisatie draait op een server in India). Wanneer is een cyber attack een casus belli, zoals bedoeld in artikel 5 van het NAVO-verdrag en artikel 51 van het VN Handvest? En hoe omgaan met collateral damage (schade aan omliggende civiele infrastructuur bij een digitale aanval)? Dit zijn onderwerpen die in een internationale context beantwoord moeten worden, bijvoorbeeld met het CCD CoE van de NAVO. Uiteindelijk zijn deze antwoorden nodig voor de Rules of Engagement voor 'onze jongens achter het beeldscherm'.
- Normatief kader voor de robuustheid van de eigen informatievoorziening. Hier komen onderwerpen aan de orde als informatiebeveiliging, risicomanagement en gewenste mate van diversiteit van het IT-landschap (hoe diverser, des te meer kans op overleven).
- Een roadmap voor de implementatie en evaluatie van deze strategie.

De volgende stap voor Defensie is ons inziens de aandacht te versterken voor cyberactiviteiten die ook externe effecten hebben, zowel defensief als offensief. Aanval is soms immers de beste verdediging en zelf offensieve vaardigheden ontwikkelen stelt de krijgsmacht ook in staat om de ontwikkelingen in de technieken voor cyber attack beter te doorgronden voor een betere verdediging van de nationale belangen van Nederland. Bijvoorbeeld door het uit kunnen schakelen van servers vanaf waar aanvallen zijn uitgeoefend op Nederlandse doelen.
We moeten echter beginnen bij het fundament. Tót de meest recente Defensie Verkenningen[9] (uit 2010) richtten strategische documenten als de Defensie Doctrine zich louter op het fysieke domein. Alleen met een zeer ruime interpretatie waren de strategische overwegingen toe te passen op cyber defence. In de Verkenningen zijn ook de ruimte[10] én cyberspace er als domein voor de krijgsmacht bijgekomen. Een noodzakelijke opfrisser in het denken over moderne oorlogsvoering en bescherming van de nationale belangen.
Opvallend is dat in alle vier de beleidsopties voor de toekomstige krijgsmacht cyber defence tot de prioriteiten behoort. Ook in zogenaamde min-varianten, waarbij van een lager defensiebudget wordt uitgegaan, blijft cyber defence staan als intensivering. Defensie komt dus uit de startblokken en moet nu overgaan naar concrete uitwerking, te beginnen met een cyberstrategie.

[9] Eindrapport Verkenningen. Houvast voor de krijgsmacht van de toekomst, ministerie van Defensie, maart 2010.
[10] Zie ook de toekomstvisie van de Koninklijke Luchtmacht, 'Het Commando Luchtstrijdkrachten in 2020-2030: moderne militaire slagkracht in de 3e dimensie', september 2009.

Beginnen met een integrale cyberstrategie

De militaire cyberstrategie van Nederland geeft aan wat Defensie moet doen om succesvol cyberaanvallen af te weren en tegenstanders in cyberspace te verslaan. De strategie moet aansluiten bij de drie hoofdtaken van Defensie, gericht op het hogere segment van het (digitale) geweldspectrum.
De taak van Defensie inzake cyber defence zou net als de 'fysieke' taakstelling drieledig moeten zijn:

1. Het beveiligen en beschermen van het nationaal relevante deel van cyberspace door continue surveillance en de inzet van cybermiddelen, een taak analoog aan de luchtverdedigingstaak van de Luchtmacht.[11]
2. Het militair optreden in cyberspace ter verdediging/bescherming van nationale en internationale belangen onder de vlag van NAVO, EU en/of VN. Het optreden als 'cyber peacekeeper' zou dus (in elk geval theoretisch) tot de mogelijkheden kunnen behoren.
3. Het ondersteunen en bijstaan van civiele instanties bij cyberaanvallen en -verdediging, onder andere met kennisdeling en bijdragen in mensen en middelen.

Cyber Power is corebusiness

Cyber defence moet gezien de eerder geschetste ontwikkelingen in cyberspace en de bedreigingen die daaruit voortvloeien voor de Nederlandse samenleving tot de kerncompetenties van onze krijgsmacht gaan behoren.
Cyber defence is niet exclusief het domein van IT of IV. De doctrinaire aanpassing, de ontwikkeling en implementatie van een cyber Concept of Operations en het ontwerpen en toepassen van processen, procedures, menskracht en technologie vormen de opmaat voor Cyber Power. Deze beschouwen we als kerncompetentie, op gelijke voet met Air, Land en Sea Power. Cyber Power kent een werkelijk 'joint' en 'combined' karakter.
Er zullen nieuwe (militaire en politieke) strategieën en tactieken nodig zijn. In hoeverre zijn concepten als 'deterrence' en 'flexible response'[12] toepasbaar? Komen we in een nieuwe wapenwedloop terecht, waarbij sprake kan zijn van een MAD 2.0?[13] Maar ook praktische vragen zullen moeten worden ingevuld, bijvoorbeeld: hoe train je voor cyber defence? Bestaat er zoiets als een digitaal oefenterrein met dezelfde uitgestrektheid en complexiteit als het World Wide Web? Het adagium 'Train As You Fight, Fight As You Train' kan dus nog een uitdaging worden. Zijn de lessen en voorbeelden uit het verleden als Von Clausewitz, Billy Mitchell en de Koude Oorlog toepasbaar?
Voor de operaties van de krijgsmacht in cyberspace is meer dan elders tenslotte realtime inzicht nodig, oftewel: cyberspace en de activiteiten die daar plaatsvinden zullen onderdeel moeten uitmaken van het Common Operational Picture en de Situational Awareness van de krijgsmacht.[14]
Cyberspace voegt al met al een geheel nieuwe dynamiek en de complexiteit toe aan de krijgsmacht en vraagt om nieuwe ideeën over deze wijze van conflictvoering.

'Gezocht: Cyber warriors (m/v)'

Door het multidisciplinaire karakter is het opstellen en operationaliseren van een cyberstrategie een complexe aangelegenheid. Onder andere politieke, juridische, militaire, psychologische en last but not least technologische factoren spelen een rol. Technologie is voor de meeste politieke en militaire leiders echter geen gemeengoed. Dit is waarschijnlijk de belangrijkste reden dat cyber defence tot dusverre beperkt van de grond is gekomen. Het vergt ook schuiven met toch al schaarse middelen vanuit een duidelijke visie.
Niet militair deelnemen aan cyberspace is in deze tijd echter geen optie meer, de recente Defensie Verkenningen leggen hiervoor de basis. Wie pakt de muis verder op?

Mike Tettero en mr. Patrick de Graaf zijn managementconsultants bij Capgemini.
Mike Tettero is gespecialiseerd in defensievraagstukken als NEC, commandovoering, cyber warfare en Information Operations.
Patrick de Graaf richt zich op strategie en innovatie van IT-organisaties in en voor de publieke sector.

[11] De Luchtmacht observeert in NAVO-verband 24 uur per dag, 7 dagen per week, het Nederlandse luchtruim met radars. Op deze wijze komt een zogenaamd 'Recognized Air Picture' tot stand, een herkend luchtbeeld dat als basis dient voor verdere tactische beslissingen zoals bijvoorbeeld de inzet van F-16's voor de onderschepping van een verdacht vliegtuig.
[12] Flexible Response is een concept binnen de NAVO, waarbij op proportionele wijze op een aanval wordt gereageerd, gebruikmakend van alle middelen in het geweldspectrum. De tegenhanger hiervan was jarenlang de doctrine van 'Massive Retaliation'.
[13] Mutually Assured Destruction (MAD), een doctrine gebaseerd op het principe van afschrikking (deterrence), waarbij een aanval op de tegenstander resulteert in zelfvernietiging.
[14] Hier ligt een geweldige technologische en cognitieve uitdaging. Hoe verkrijg je actueel inzicht in eventuele bedreigingen met vele miljoenen computersystemen en netwerken en potentieel miljarden gebruikers? Dreigingsanalyses en 'intelligence' zijn essentieel.

3 Vitale infrastructuren op weg naar volwassenheid

Invulling veiligheid bij vitale sectoren meer op basis van zelforganiserend vermogen.

Drs. Joep Cremers
Drs. Melle van den Berg

Vitale sectoren, zoals de energie- en drinkwatersector hebben een verantwoordelijkheid in het waarborgen van continuïteit van essentiële levensbehoeften en maatschappelijke processen. Sinds 9/11 hebben deze sectoren, mede door nieuwe initiatieven van de overheid op het gebied van veiligheid, invulling gegeven aan deze verantwoordelijkheid. Deze overheidsinitiatieven lijken echter ook de eigen invulling van verantwoordelijkheden vanuit de vitale sectoren te belemmeren. Zo lijken de vitale sectoren te verdwalen in het totaal aan nieuwe overlegstructuren die in het leven zijn en worden geroepen. In dit hoofdstuk betogen wij dat deze ontwikkeling op den duur niet effectief is. Vitale sectoren zouden op basis van zelforganiserend vermogen invulling moeten geven aan deze verantwoordelijkheid. De rol van de overheid richt zich daarbij op een van regisseur en systeemverantwoordelijke.

Security en veiligheid op de kaart bij vitale sectoren

In de afgelopen jaren heeft het securitybeleid rondom de vitale infrastructuur in Nederland vorm gekregen. Nadat in 2002 voor het eerst een overzicht werd gemaakt van alle sectoren die vanuit economisch perspectief vitaal zijn, is in 2005 een eerste aanzet gemaakt tot een actieprogramma voor deze sectoren. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) had daarin een coördinerende rol door het starten van het Programma Bescherming Vitale Infrastructuur. In Den Haag stond hiermee het garanderen van veiligheid en continuïteit van vitale processen op de politieke agenda.

De vitale sectoren

- Energie
- Telecommunicatie/ICT
- Drinkwater
- Voedsel
- Gezondheid
- Financieel
- Keren en beheren oppervlaktewater
- Openbare orde en veiligheid
- Rechtsorde
- Openbaar bestuur
- Transport
- Chemische en nucleaire industrie

Bron: Rapport bescherming vitale infrastructuur, ministerie van BZK, 1 september 2005

Mede door de terroristische aanslagen in onder andere Madrid en Londen kwam veiligheid nog hoger op de politieke agenda te staan. Met die aandacht voor veiligheid werden er ook andere initiatieven gestart om de samenleving weerbaarder te maken en de respons op een mogelijk terroristische aanslag effectief te laten zijn. Niet alleen vanuit het oogpunt van continuïteit van essentiële levensbehoeften, maar ook vanuit invalshoeken als terroristische dreigingen en het bezit van chemische, biologische, radiologische of nucleaire stoffen werden organisaties in de vitale sectoren benaderd. Kortom, een groot deel van deze initiatieven raakten de vitale sectoren. De periode vanaf 2002 tot 2010 kan als de opstartfase worden gezien, waarin veiligheid en security nadrukkelijk bij een groot aantal vitale sectoren op de agenda is komen te staan. In deze periode zijn sectoren aangesproken om zich te organiseren en hebben de ingevoerde maatregelen in veel gevallen geleid tot

Een overzicht van initiatieven voor vitale sectoren

- Programma Vitaal
- Grieppandemie
- Chemische, radiologische, biologische en nucleaire weerstandsverhoging
- Alerteringssysteem Terrorisme-bestrijding
- Grootschalige oefeningen zoals Voyager en Waterproef
- Convenanten en afstemming met veiligheidsregio's en gemeentes
- Information Sharing and Analysis Centers (ISACs) via het NICC (Nationale Infrastructuur voor de Bestrijding van Cybercrime)
- Brancheoverleggen, zoals het Nationaal Continuïteitsoverleg Telecom (NCO-T) en Business Continuity Vitale Infrastructuur Financiën (BC-VIF)
- European Programme for Critical Infrastucture Protection (EPCIP) en Critical Information
- Infrastructure program (CIIP)
- Strategisch overleg vitale infrastructuren (SOVI)
- Nationaal Adviescentrum Vitale Infrastructuur (NAVI)
- Securitymanagementsystemen
- C2000-beveiligingsplannen
- Eenheid planning en advies
- ICT Response Board

vruchtbare samenwerking en afstemming. Juist de benadering van het thema veiligheid vanuit veel invalshoeken heeft ertoe geleid dat de Nederlandse overheid actief werk maakt van veiligheid en de veiligheid van de vitale infrastructuren in het bijzonder.

Deze aanpak kent ook nadelen. Zowel voor de overheid als voor de betrokken sectoren is het een intensieve en tijdrovende exercitie om weerbaar en paraat te zijn. De veelvoud aan gremia en initiatieven leidt tot veel overleg. In dat web van overlegstructuren is de samenhang niet altijd duidelijk, hetgeen ten koste gaat van duidelijkheid, helderheid en een integrale aanpak.

Een veelvoud aan initiatieven

Veiligheid wordt serieus genomen en er is ook veel gedaan om veiligheid bij vitale sectoren te verhogen. Een veelvoud aan initiatieven is opgestart om het weerstandsvermogen te verhogen en een effectieve respons in geval van incidenten te verbeteren. Een greep uit deze initiatieven staat in het kader hiernaast.

Hoewel niet elk van deze initiatieven van toepassing is op ieder vitaal bedrijf, zijn er organisaties te noemen die op enige manier bij driekwart van deze initiatieven betrokken zijn. Daarbij moet worden gezegd dat een deel van de initiatieven uit eenzelfde koker komt en daarmee ook is afgestemd. Maar er zijn ook trajecten die meer als een losstaand initiatief worden uitgevoerd. De timing van deze verschillende trajecten is echter niet op elkaar afgestemd, afstemming tussen de organiserende partijen ontbreekt. Dit heeft tot gevolg dat een vitaal bedrijf met verschillende partijen spreekt over het

thema veiligheid en dat discussies niet altijd op elkaar aansluiten. Elk van deze initiatieven levert op zichzelf een waardevolle bijdrage aan een veilige maatschappij.

Wanneer deze initiatieven echter uiteindelijk door eenzelfde vitaal bedrijf worden opgepakt, is er een gevaar dat het overzicht ontbreekt. Een vitaal bedrijf vraagt zich af hoe deze initiatieven samenhangen en of ze niet met minder gremia af zouden kunnen. Samengevat: er wordt een programma beveiliging vitale infrastructuur in het leven geroepen. De sectoren definiëren maatregelen en gaan serieus aan de slag om die maatregelen te implementeren. Wanneer dat is gedaan, denkt de organisatie daarmee te voldoen aan landelijke normen en het daarmee in zekere zin goed geregeld te hebben. Maar nieuwe initiatieven brengen met zich mee dat net ontwikkelde procedures niet meer aansluiten. Dit kan op den duur tot frustratie leiden en ten koste gaan van een welwillende houding.

De overheid zou zich om de vitale sector heen moeten organiseren. Deels is dat wellicht een utopie, omdat er afstemming op lokaal, regionaal, nationaal en EU-niveau plaats dient te vinden. Maar het duidelijker met één stem spreken vanuit 'Den Haag' is daarin wel een belangrijke stap.

Het zou echter te gemakkelijk zijn om slechts kritische geluiden te laten horen over de vele overheidsinitiatieven op het gebied van veiligheid. Deze versnipperde impulsen zijn nodig geweest en hebben binnen de organisaties in de vitale sectoren daadwerkelijk een proces in beweging gezet. Vaak was bij aanvang van al deze initiatieven nog geen securitymanager of een vergelijkbare functie benoemd. En ook waar deze bedrijfsfunctie inmiddels wel is ingericht, is dat nog geen garantie dat de medewerkers die actief zijn op het vlak van veiligheid elkaar weten te vinden en acties afstemmen. Zo kan de verantwoordelijkheid binnen de organisatie versnipperd zijn, zoals wanneer één groep medewerkers verantwoordelijk is voor het oefenen van de crisisorganisatie, een andere afdeling zich bezighoudt met ICT-security en weer een andere groep toegangsbeleid en bouwtechnische maatregelen doorvoert. De kunst is om al die maatregelen als onderdeel van een integrale aanpak op veiligheid vorm te geven. Dat geldt dus zowel binnen het vitale bedrijf als bij de overheid die iets van dat vitale bedrijf wil.

Veel actie, weinig samenhang

Als resultante van al deze initiatieven zijn de vitale organisaties veel tijd kwijt met afstemming, het opstellen van convenanten, elkaar leren kennen, afhankelijkheden onderzoeken en samenwerking oefenen. Wat in toenemende mate belangrijk wordt, is de vraag hoe daar het meest handig invulling aan te geven. Voor een deel zijn deze taken een permanent onderdeel van hun pakket. De praktijk leert dat wanneer een onderwerp geen topprioriteit meer heeft, er minder middelen en tijd beschikbaar zijn. Zo is in diverse vitale sectoren de beleving dat de projectfase 'vitaal' voorbij is, waardoor er geen middelen en tijd meer beschikbaar zijn.

Zowel de vitale sectoren als beleidsdirecties staan voor de uitdaging om de slag te maken van het opstarten van initiatieven naar het duurzaam, effectief en integraal borgen van veiligheid

in de vitale sectoren. Vraag is hoe die borging dan moet plaatsvinden. Daarbij is het zaak kritisch te kijken naar de rol van de vitale sectoren enerzijds en die van beleidsmakers anderzijds.

Zelforganiserende vitale sectoren als uitgangspunt

De verantwoordelijkheid voor een vitaal proces ligt in de eerste plaats bij het vitale bedrijf zelf. Een internetprovider moet bijvoorbeeld hebben nagedacht hoe de beschikbaarheid van het internet kan worden gegarandeerd en wat er moet gebeuren bij een incident. Een drinkwaterbedrijf is verantwoordelijk voor leveringszekerheid. Dus onafhankelijk van de vele externe initiatieven ligt de primaire verantwoordelijkheid voor invulling en uitvoering bij het vitale bedrijf.
Een bedrijf wil 'in control zijn': veiligheidsrisico's in beeld hebben, daar bewust en aantoonbaar afwegingen over gemaakt hebben, controleerbare maatregelen uitgevoerd hebben en liefst ook nog de effectiviteit ervan toetsen. Deels vanwege de wensen uit de buitenwereld, waaronder overheden, maar grotendeels vanuit de eigen verantwoordelijkheid die een organisatie binnen een vitale sector voelt.

Om deze verantwoordelijkheid vorm te geven is in ieder geval betrokkenheid van het management randvoorwaardelijk. Maar ook praktische zaken moeten geregeld zijn: wie herziet periodiek de risicobeoordeling en wordt daarin dan meegenomen welke ketenafhankelijkheden en relaties met andere vitale sectoren er zijn? Heeft een organisatie een eigen oefenbeleid en acteert zij daarop, of vinden multidisciplinaire oefeningen alleen plaats als een veiligheidsregio daartoe uitnodigt? Zijn er waakvlamovereenkomsten met leveranciers om in crisistijd over materialen of diensten te kunnen beschikken? Allemaal voorbeelden hoe een organisatie door grip op haar eigen processen ook grip op de omgeving kan krijgen. Door over dit soort vragen intern na te denken en extern te handelen kan feitelijk invulling gegeven worden aan het zelforganiserende vermogen van vitale sectoren. Juist door deze aspecten expliciet bij een vitaal bedrijf te beleggen wordt geappelleerd aan de eigen verantwoordelijkheid van de organisatie.
Wanneer een vitale organisatie de interne besturing omtrent veiligheid goed regelt, straalt ze vertrouwen uit naar externe partijen. In het samenspel tussen vitale sectoren en overheden is het erg belangrijk aantoonbaar grip op de situatie te hebben om zo vertrouwen te kweken. Dat biedt dan ook aanknopingspunten voor een faciliterende overheid met een regierol.

Regierol overheid

De overheid staat voor het behartigen van het landsbelang en is daarmee op nationaal niveau verantwoordelijk voor de vitale infrastructuren. Op dit moment zijn er wel dergelijke overlegstructuren, maar is er ook echt een partij die als regisseur optreedt? En hoe is de toezichthoudende functie ingevuld?

Voor de overheid ligt een aantal duidelijke structurele uitdagingen in de manier waarop de beveiliging van de vitale infrastructuur is opgezet. De projectfase is over: het programma Bescherming Vitale Infrastructuur is opgeheven. Ook het Nationaal Adviescentrum Vitale Infrastructuren (NAVI) is opgehouden te bestaan. En op het vlak van terrorisme heeft de

NCTb de regie. Voor ICT-incidenten blijft de verdeling van taken en verantwoordelijkheden een heikel punt. En hoe de ontwikkelingen van Europese regelgeving een effect hebben op de relatie met de vitale sectoren blijft ook nog deels gissen.

Op dit moment is onduidelijk op welke gronden vitale sectoren gehouden kunnen worden aan gemaakte afspraken. Dit is een rechtstreeks voortvloeisel van de manier waarop de aansturing op het gebied van vitale infrastructuren is opgezet: veelal in publiek-private samenwerking als een netwerk. Dit hoeft geen belemmering te vormen om afspraken te formuleren die helderheid scheppen, mits de overheid duidelijke kaders schept waarbinnen deze afspraken tot stand komen.

Tot slot

In dit betoog hebben we aangegeven dat de taakverdeling binnen en het veelvoud aan overleggen over vitale infrastructuren nader overwogen dienen te worden, aangezien de huidige aanpak onvoldoende integraal en effectief is.

Belangrijk daarbij is verantwoordelijkheid neer te leggen op de plaats waar dit het meest voor de hand ligt. In het geval van vitale infrastructuur is dat op de eerste plaats de vitale organisatie zelf. Zij heeft een taak om - in 'vredestijd en in oorlogstijd' - de levering van haar diensten te garanderen. Daarvoor is intern een professionele aanpak van veiligheid en beveiliging nodig, voordat in het ecosysteem van betrokken organisaties een vitaal bedrijf wensen of eisen kan stellen.
Daarnaast is er de overheid, die er groot belang bij heeft dat vitale infrastructuren blijven functioneren en daarmee meer een rol als systeemverantwoordelijke heeft. Uitdaging is om zo veel mogelijk als één overheid richting de vitale infrastructuren op te treden en daarbij het landsbelang boven ministeriële verantwoordelijkheid te stellen.

Drs. Joep Cremers en drs. Melle van den Berg zijn managementconsultants bij Capgemini.
Joep Cremers is gespecialiseerd in organisatie- en bedrijfsvoeringsvraagstukken in het veiligheidsdomein.
Melle van den Berg heeft zich gespecialiseerd op bescherming van overheidsdata en de definitie van vitaal binnen en buiten de overheid.


Attentie
Buurtpreventie

4 Veiligheid, wat moet ik ermee?

Drs. Nicole de Ridder
Drs. Roy Oudeman

Vragen die burgers met enige frequentie beantwoord willen zien, zijn: Hoe is het gesteld met de veiligheid in mijn leefomgeving? Had ik wat moeten doen toen die jongen op straat in elkaar werd geslagen? Wat kan ik aan mijn veiligheid doen? Wat doet de overheid om mijn veiligheid te bewaken? En dit is nog maar een kleine selectie aan veiligheidsvraagstukken. Wat vertellen zij ons?

In dit hoofdstuk wordt beschreven hoe de burger in Nederland heden ten dage worstelt met het onderwerp veiligheid. De (on)veiligheidsgevoelens zijn kenmerkend voor de moderne samenleving en worden gevoed door de actuele informatie die voor eenieder over dit onderwerp verkrijgbaar is. Nu de overheid inziet dat zij niet in staat is om op geheel eigen kracht het veiligheidsprobleem te lijf te gaan, wordt een actievere rol van de burger verwacht. Dit maakt de situatie voor de burger nog ingewikkelder.

In dit hoofdstuk zullen wij aantonen dat een grote groep burgers participeert in projecten waarin hij als coproducent optreedt en dat deze initiatieven ook daadwerkelijk bijdragen aan een veiliger samenleving. Om met succes door te kunnen pakken op deze trend is de benaderingswijze van de overheid van groot belang. De rol van de overheid dient zo ingericht te worden dat de burger effectief als coproducent kan optreden. Niet alle groepen burgers zijn echter gemakkelijk te bereiken en er is sprake van een constructieve, passieve dan wel defensieve houding. Het is daarom ondoenlijk om met één strategie alle groepen te bereiken. Desalniettemin dient de overheid ruimte te creëren voor de burger om eigen verantwoordelijkheid te nemen om zo de rol van de burger als coproducent van veiligheid in de samenleving te verankeren.

Voeding onveiligheidsgevoelens

Het is kenmerkend voor onze moderne samenleving dat ontwikkelingen zich razendsnel en, voor het gevoel van de burger, buiten hun invloedssfeer afspelen. Geconfronteerd met deze onzekerheden worden risico's angstvallig gemeden en liggen veiligheidszaken buitengewoon gevoelig. Deze angst wordt gevoed door verschillende bronnen. Een van de bronnen is de beschikbare, actuele informatie over veiligheidszaken via de media, internet en andere (technologische) ontwikkelingen. Gesteld kan worden dat over het algemeen negatieve informatie over veiligheid via de media ontsloten wordt. Deze haalt immers eerder de krantenkoppen. Denkt u hierbij aan een lichaam van een vrouw die levenloos is gevonden op het strand; een familiedrama waar de vader zijn vrouw en kinderen heeft vermoord; een situatie waar op klaarlichte dag op een fietser is geschoten, maar ook berichten over gewelddadige inbraken; autodiefstallen en vandalisme. Dit zijn allemaal geen uitzonderlijke berichten.

Naast deze informatie worden jaarlijks landelijke en gemeentelijke cijfers bekendgemaakt over de veiligheidssituatie. Voorbeelden hiervan zijn de Misdaadmeter van het Algemeen Dagblad en de Integrale Veiligheidsmonitor. De belangrijkste resultaten van de Integrale Veiligheidsmonitor in 2008 zijn bijvoorbeeld:

- geen verdere daling van de onveiligheidsgevoelens. Dit betekent dat een kwart van de bevolking zich weleens onveilig voelt;

- licht dalende trend van het slachtofferschap van veel voorkomende criminaliteit;
- inwoners zijn vooral slachtoffer in de eigen woonomgeving;
- het gevoel van onveiligheid in de eigen buurt gaat vooral samen met criminaliteit en andere buurtproblemen.

De conclusies van de Integrale Veiligheidsmonitor vormen alleen al voldoende voedingsbodem voor de burger om zich onveilig te voelen, voornamelijk in de eigen leefomgeving. Daarnaast worden dit soort cijfers ook nog versterkt door de frequente berichtgeving in de media over onveilige situaties. De burger heeft zo meer dan voldoende informatie waardoor hij zich in toenemende mate onveilig voelt.

Verschuivingen in verantwoordelijkheden veiligheidszorg

Op dit moment vinden verschuivingen plaats omtrent de verantwoordelijkheden rond de veiligheidszorg. Waar de centrale overheid voorheen de veiligheidszorg steeds verder naar zich toetrok, is nu een kentering te zien. Overheidsinstanties en hulpdiensten beseffen dat zij vaak niet in staat zijn om veiligheidskwesties alleen op te lossen. Politie en justitie hebben een beperkt aantal instrumenten en niet altijd toereikende capaciteit. Daarnaast spelen diverse kerntakendiscussies, bezuinigings- en heroverwegingsrondes een rol. Mede hierdoor krijgt de burger zelf meer verantwoordelijkheid toegedicht en wordt een actieve bijdrage aan een veiligere samenleving verwacht. De burger als coproducent. Deze nieuwe rol zorgt voor verwarring bij de burger. Er wordt geworsteld met de vraag hoe die rol ingevuld kan worden. Naast deze actieve burger, de coproducent, is er ook een groep burgers die zich een zelfstandige rol in het veiligheidsdomein toe-eigent. Zij zijn ontevreden over de resultaten die overheidsinstanties op veiligheidsgebied boeken en treden zelf op tegen bijvoorbeeld criminaliteit in de buurt. Goed voorbeeld zijn de bordjes 'Buurtpreventie' die hier en daar in steden eigenhandig worden opgehangen.

De burger als coproducent

De burger als coproducent kent vele verschillende verschijningsvormen. Twee expliciete rollen, die van informant en medewerker, werken we hier verder uit.

Informant

De burger wordt door de overheid en hulpdiensten uitgenodigd om informatie te leveren die bijdraagt aan een veiligere samenleving. Burgernet en SMS-Alert zijn voorbeelden waarbij de burger ingezet wordt als extra oren en ogen bij de opsporing. Bij SMS-Alert kan de burger zichzelf aanmelden waarna het per sms berichten ontvangt over incidenten die plaatsvinden in hun directe omgeving. Een voorbeeld van een incident is een inbreker die op de vlucht is. SMS-Alert richt zich op veiligheid in zeer lokaal en fysiek gebonden gebieden. Voor de opsporing op landelijk niveau worden andere instrumenten ingezet om de burger als informant te raadplegen: bijvoorbeeld het tv-programma Opsporing Verzocht en Meld Misdaad Anoniem. Meld Misdaad Anoniem is inmiddels zeer succesvol, blijkens de jaarcijfers 2009 uit het persbericht van Meld Misdaad Anoniem (www.meldmisdaadanoniem.nl).

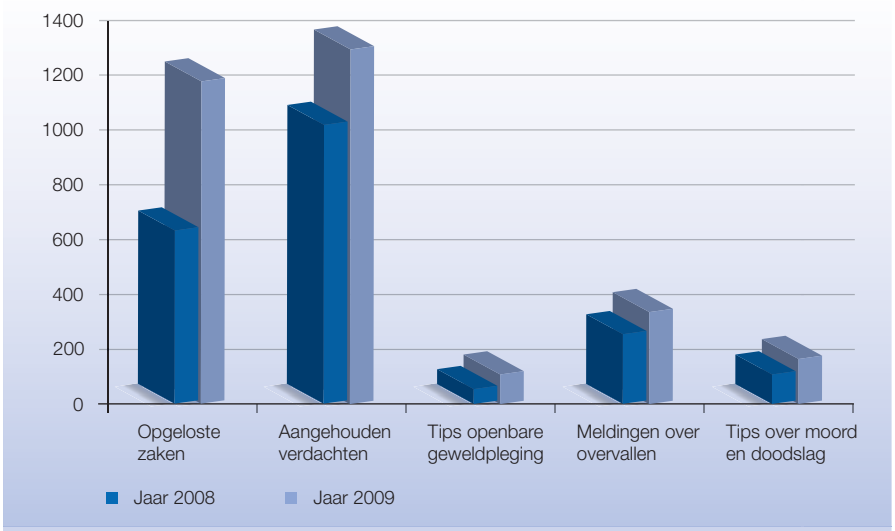
Medewerker

Naast de rol van informant wordt de burger bij zeer diverse initiatieven be-

trokken waar hij als medewerker wordt ingezet bij het werken aan een veiligere samenleving. Hier kan worden gedacht aan initiatieven op lokaal niveau om de directe leef- en woonomgeving veiliger te maken, zoals buurtbemiddeling, buurtvaders en gedragscodes. Bij gedragscodeprojecten maken bewoners afspraken met elkaar om de onderlinge band te verstevigen, de betrokkenheid bij de eigen buurt te vergroten en het veiligheidsgevoel te verhogen. De afspraken komen in de wijk te hangen en een van de afspraken is dat bewoners elkaar aanspreken op de naleving van de afspraken.
Een voorbeeld op landelijk niveau van waar de burger als medewerker wordt ingezet, komt tot uiting in de campagnes van de overheid waarin de burgers worden geïnformeerd hoe om te gaan met het zien van geweld, zonder zichzelf in gevaar te brengen. De vier acties zijn: mobiliseer omstanders; bel het alarmnummer 112; onthoud de kenmerken van de dader en laat het slachtoffer niet alleen. Daarnaast wordt de burger actief benaderd bij vermissing van kinderen door middel van Amber Alert. Dit overigens alleen indien de burger zichzelf daartoe heeft aangemeld.
Naast het meewerken aan een veilige leef- en woonomgeving wil de overheid de burgers ook stimuleren om zelfredzaam te zijn wanneer het gaat om veiligheid. Een voorbeeld hiervan is de 'Denk Vooruit'-campagne waarin de overheid aangeeft dat hulpinstanties niet altijd iedere burger direct kunnen helpen en het dus noodzakelijk is dat burgers zelfredzaam zijn.

Bovenstaande cijfers en voorbeelden geven aan dat de inzet van burgers in deze gevallen succesvol is bij het werken aan een veiligere samenleving.

Jaarcijfers 2009 Meld Misdaad Anoniem



Bron: Meld Misdaad Anoniem jaarverslag 2009 op http://www.meldmisdaadanoniem.nl

Daarnaast blijkt daaruit dat bij een groep burgers bereidheid bestaat tot participatie. De initiatieven waar burgers bij betrokken worden, zijn de afgelopen jaren alleen maar toegenomen en er is geen reden om aan te nemen dat dit in de toekomst minder wordt. De burger ziet dus een toenemende vraag vanuit de overheid en hulpdiensten om te helpen bij het veiliger maken van de samenleving en een deel van de burgers beantwoordt die vraag positief.
Tot zover kan worden geconcludeerd dat de burger wordt geconfronteerd met een terugtrekkende overheid, de vraag om hulp bij het werken aan een veilige samenleving en tegelijkertijd met toenemende gevoelens van onveiligheid. Wat doet u? U voelt zich onveilig en er wordt in toenemende mate een beroep op u gedaan om de samenleving veiliger te maken. Een deel van de bevolking blijkt bereid te zijn om mee te werken, de zogeheten constructieve houding.

Constructieve houding

In dit geval kiest de burger ervoor om, ondanks onzekerheden over veiligheid, constructief mee te werken aan het veiliger maken van de samenleving. Op landelijk en lokaal niveau ontbreekt het aan cijfers over de omvang van het aantal burgers dat participeert in initiatieven ten behoeve van een veilige samenleving.

Een kleine indicatie geven de cijfers van specifieke projecten zoals Meld Misdaad Anoniem, Buurtbemiddelingsprojecten en SMS-Alert. In 2009 zijn per week 130 tips doorgegeven aan Meld Misdaad Anoniem door participerende burgers.

Het aantal vrijwilligers bij Buurtbemiddelingsprojecten is de afgelopen jaren ook sterk toegenomen. Inmiddels zijn er meer dan 150 projecten met gemiddeld tien vrijwilligers. Per gemeente zijn er cijfers bekend over het aantal aanmeldingen voor SMS-Alert. Het aantal aanmeldingen hangt natuurlijk af van het aantal bewoners per gemeente, maar ligt voor deelnemende gemeenten tussen de 5.000 en 10.000 aanmeldingen. In november 2009 hebben de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Justitie besloten tot de verdere landelijke uitrol van Burgernet. Met deze beslissing wordt SMS-Alert ook landelijk uitgerold, omdat dit gekoppeld wordt aan Burgernet. Burgernet is een samenwerkingsverband tussen burgers, gemeente en de politie om de veiligheid in woon- en werkomgeving te bevorderen op eenzelfde wijze als SMS-Alert. Stel we extrapoleren, op basis van de landelijke uitrol, het gemiddeld aantal aanmeldingen SMS-Alert per gemeente (5.000), dan komen we op een totaal van 2.155.000 actieve burgers. Interessant zou zijn om alle initiatieven waarbij burgers betrokken zijn om de samenleving veiliger te maken, te bekijken. Bovenstaande aantallen zijn namelijk gebaseerd op slechts drie initiatieven.

Een deel van de bevolking heeft deze constructieve houding. Welke houding neemt de rest van de bevolking aan ten opzichte van de veiligheidsvraagstukken waarvoor zij zich geplaatst ziet? In de volgende alinea's worden twee andere houdingen van de burgers toegelicht: de defensieve en passieve houding.

Defensieve houding

Een bepaalde groep burgers is zich door de worsteling met (on)veiligheidsgevoelens zelfstandig gaan verdedigen. Dit zijn vaak de ontevreden burgers die het heft in eigen hand nemen bij het optreden tegen criminaliteit en daarbij niet samenwerken met overheidsinstanties. De defensieve houding voert in Nederland gelukkig (nog) niet de boventoon, maar in het buitenland kent men bijvoorbeeld al de zogenaamde 'gated community'. Dit zijn woongemeenschappen waar door middel van hekken en grachten de toegang is beperkt. Ook in Nederland lijken vormen van 'gated communities' in opmars, zoals nieuwbouwwijken met omliggende grachten en één centrale toegangspoort.

Voorts wordt ter bescherming van de eigen woon- en leefomgeving in diverse landen om bijna ieder huis een hek geplaatst, bewakingshonden aangeschaft en een lidmaatschap bij een particuliere beveiliging aangegaan. Een andere vorm van zelfbescherming is het aanschaffen van geweren en pistolen, waarmee de familie en het eigen bezit beschermd kan worden. Of beveiligers/bodyguards/chauffeurs worden ingehuurd ter bescherming. Nu lijkt dat voor Nederland nog toekomstmuziek, maar ook hier laten de welgestelde medeburgers steeds vaker een 'panic room' inbouwen. Dit is een versterkte kamer in huis met extra beveiligingsmaatregelen en communicatiemiddelen waar de bewoners naartoe kunnen vluchten bij inbraak of overval.

Passieve houding

De laatste houding die burgers kunnen hebben in relatie tot veiligheid is dat zij niets doen. Deze houding

kan ingegeven worden door verschillende motieven. Een deel van de burgers ervaart wel onveiligheidsgevoelens, maar acht de kans zeer klein dat hen wat overkomt. Doordat de kans zo klein wordt ingeschat, zijn zij niet geneigd om iets te ondernemen. Andere burgers zijn zeer op zichzelf gericht en vinden dat zij zichzelf kunnen redden en verder geen bijdrage hoeven te leveren aan de maatschappij: 'ze betalen tenslotte belasting'. De verantwoordelijkheid voor veiligheid is die van de overheid en de hulpdiensten. Ook zijn er burgers die onveiligheidsgevoelens ervaren, maar niet weten hoe zij een goede bijdrage kunnen leveren. Wat kan de overheid met deze verschillen tussen burgers en motieven in hun verstandhouding tot veiligheidsvraagstukken?

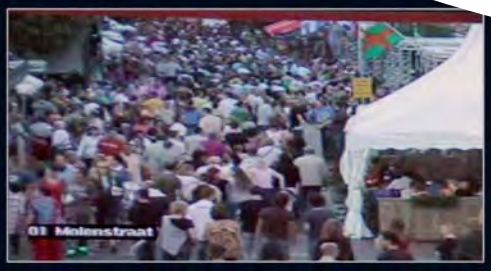
Huidige rol overheid en hulpdiensten

De rol van de overheid en de hulpdiensten moet worden aangepast, zodat zij kunnen faciliteren bij hun toenemende wens om de burger als coproducent van veiligheid op te laten treden. In ieder geval is het niet mogelijk om met één strategie in te spelen op de verschillende houdingen en motieven van de burgers. De houdingen bieden vooral inzicht en als overheid wil je voorkomen dat het aantal defensieve en passieve burgers gaat toenemen. Burgers ervaren hun relatie tot (on)-veiligheidsgevoelens, de vragende overheid om hen te betrekken bij het creëren van een veilige samenleving en de terugtrekkende overheid op hun eigen manier. Wat zorgt ervoor dat de burgers zich bij deze worsteling ontpoppen tot constructieve burgers? Op dit moment worden de burgers met verschillende boodschappen en op verschillende wijzen benaderd. De ene communicatiestrategie is erop gericht om de burgers te informeren over de risico's en handelingsperspectieven aan te dragen. Denk hierbij aan de kaartjes die door de politie zijn verstrekt om in de auto te leggen met de boodschap voor potentiële inbrekers dat de auto al leeg is. Aan de andere kant worden burgers soms bewust niet geïnformeerd over onveilige situaties. Ook de wijze waarop burgers geïnformeerd en benaderd worden, is zeer divers: via landelijke campagnes, buurthuizen, brieven van de gemeente en bewonersbijeenkomsten. Welke strategie nu effectiever is dan de andere, is niet duidelijk. Wel is bekend dat de ene strategie beter aansluit bij de ene burger dan bij de andere. Het lijkt tot dusver niet nodig om met bepaalde middelen te stoppen en de nadruk op één enkele strategie te leggen.

Ruimte creëren

De voorbeelden in voorgaande alinea's tonen aan dat er voldoende succesvolle initiatieven met inzet van burgers zijn. Daarnaast blijkt een groep constructieve burgers bereid om aan een veiligere samenleving mee te werken. Op basis van deze constateringen is het goed om de inzet van de burger als coproducent van veiligheid door te zetten. Om deze trend uit te breiden en te verankeren in de samenleving, dient er vanuit de overheid en hulpdiensten nog meer ruimte te worden gecreëerd voor de burger om eigen verantwoordelijkheid te kunnen nemen. Geef een deel veiligheidszorg verder terug. Maak deze focus ook expliciet duidelijk in de communicatie naar de samenleving. Op deze manier laten ze zien vertrouwen te hebben in de burger en deze serieus te nemen in het samenwerken aan een veilige samenleving.

Dit geconcludeerd hebbende heeft het creëren van ruimte voor de burger een bijkomstig voordeel dat op termijn de overheid en hulpdiensten ook ruimte voor zichzelf kunnen creëren. De overheid en hulpdiensten kunnen zich bijvoorbeeld gaan richten op de minder zelfredzame groeperingen in Nederland. De vraag is nu of de overheid daadwerkelijk de ruimte durft te laten aan de burger om eigen verantwoordelijkheid te nemen.



01 Molenstraat

02 Ziekerstraat

03 Koningsplein

06 Hertogstraat

07 Hertogplein

08 Hunnerpark

11 Holland Casino

12 Waalkade

13 Labyrinth

5 Veiligheidshuizen: bureaucratische theekrans of doelmatige coördinatie!?

Naar een toekomst zonder onnodige vervlechting en bureaucratie.

Drs. Dennis van Breemen
Drs. Wender van Mansvelt

"Veiligheidshuizen bieden een mogelijkheid tot samenwerken waar wij vroeger alleen van konden dromen. Laten we er daarom optimaal gebruik van maken en samen bouwen aan een veilige toekomst."
E.M.H. Hirsch Ballin

De Veiligheidshuis-formule

December 2009 was een mijlpaal. Op dat moment had Nederland een landelijk dekkend netwerk van vijfenveertig Veiligheidshuizen gerealiseerd. De jongste cijfers geven aan dat er daadwerkelijk resultaten geboekt worden: recidive cijfers nemen af, evenals de absolute criminaliteitscijfers en onveiligheidsgevoelens in de buurten. De aanpak smaakt naar meer: in de Veiligheidskrant geeft de staatssecretaris aan dat de komende tijd in het teken zal staan van doorontwikkeling van de Veiligheidshuizen. Een van die doorontwikkelingen is het nadrukkelijker betrekken van zorg en onderwijs en het daarmee versterken van de regionale functie van het Veiligheidshuis (Veiligheidskrant).
Toch worden er ook andere geluiden gehoord. Veiligheidshuizen als instituties introduceren het risico op een nieuwe vorm van bureaucratie. Door de lokale aanpak ontstaat een wildgroei van procedures, informatie-uitwisseling en systemen die zich veelal moeizaam verhouden met de efficiënte en (landelijke) uniforme inrichting van de eigen organisatie. Kortom: de spanning tussen een efficiënte backoffice en een flexibele frontoffice.
Wij denken dat de invoering van deze Veiligheidshuis-formule echt een gouden greep is geweest. Ondanks de reeds behaalde successen zal men, 'om er optimaal gebruik van te kunnen blijven maken', niet enkel naar de succesfactoren moeten kijken, maar tevens de nog aanwezige obstakels moeten onderkennen om de continuïteit van de veiligheidshuizen te garanderen en de aanpak verder te verbeteren.

Om deze Veiligheidshuis-formule in stand te houden is het van wezenlijk belang om uit te stijgen boven het niveau van 'best practice' en de achterliggende mechanismen, die maken dat het werkt, te doorgronden. Alleen dan wordt men in staat gesteld diezelfde mechanismen, waar nodig, bij te stellen, aan te passen aan de veranderende omgeving en robuust te maken. Wij stellen dat de Veiligheidshuis-formule momenteel en naar de toekomst toe zeer kwetsbaar is en onderhavig aan legio factoren die zijn waarde sterk kunnen beïnvloeden. Een van die factoren is de mate van samenwerking, het maken van afspraken onderling en de afstemming tussen verschillende organisaties.

In dit essay geven wij aan wat wij zien als de drie belangrijkste uitdagingen voor de Veiligheidshuizen als geheel en voor de individuele organisaties binnen dit samenwerkingsverband. Allereerst geven we een korte beschrijving van het Veiligheidshuis, dan volgt een overzicht van huidige trends en risico's. Afsluitend bespreken wij vier gouden tips die het Veiligheidshuis robuuster maken en de huidige succesfactoren binnen de doorontwikkeling borgen.

Wat is een Veiligheidshuis?
Een Veiligheidshuis is een netwerkorganisatie waar verschillende instanties op één locatie samenwerken om maatschappelijke problemen (met name: openbare orde, jeugdcriminaliteit, veelplegers en huiselijk geweld) het

hoofd te bieden. Centraal binnen het Veiligheidshuis staat de persoonsgerichte aanpak via het casusoverleg. Doel is dat de ketenpartners gezamenlijk problemen signaleren, analyseren en oplossingen bedenken om deze vervolgens samen uit te voeren. Werkprocessen worden op elkaar afgestemd, zodat strafrecht en zorg elkaar aanvullen in plaats van elkaar, vanuit de eigen aanpak en overtuiging, ongewild dwarsbomen. Dankzij deze aanpak komt de verdachte, crimineel of overlastgevende jongere, 'de klant' centraal te staan. Alle betrokken partijen voeren gezamenlijk overleg om zo te komen tot één sluitende aanpak of behandelplan. Deze integrale aanpak waarbij repressie en zorgverlening op elkaar worden afgestemd, levert momenteel al veelbelovende resultaten op (voortgangsrapportage VbbV oktober 2009).

Trends, ontwikkelingen en risico's

De kracht van de Veiligheidshuisformule is gelegen in de netwerkstructuur: verschillende netwerken uit de bestuurlijke, strafrechtelijke en zorginstellingen, die samenwerken om de aanpak van criminaliteit en overlast beter op elkaar af te stemmen. Op dit moment is er sprake van een landelijk dekkend netwerk van Veiligheidshuizen. In negenenveertig grote en middelgrote steden is momenteel een Veiligheidshuis ingericht. Aangegeven wordt dat het komende jaar in het teken staat van continuïteit en borging, van doorontwikkeling van de Veiligheidshuizen en het beter op elkaar laten aansluiten van de (lokale) zorg en de strafrechtelijke aanpak.

Ten aanzien van continuïteit en borging geeft men aan dat het uitdrukkelijk niet de bedoeling is om te streven naar één uniforme blauwdruk voor alle Veiligheidshuizen. Toch blijkt dat er bij bepaalde organisaties juist wel de behoefte bestaat aan een landelijke richtlijn die hun rol sterk maakt voor de toekomst. Dit geldt met name voor de meer centraal aangestuurde (landelijke) organisaties zoals bijvoorbeeld het Openbaar Ministerie, de Raad voor de Kinderbescherming en de politie. Standaardisatie is voor deze instanties van belang voor het beschrijven van functieprofielen, het faciliteren van ICT-voorzieningen, rapportagelijnen en opschalingsprotocollen. Op dit moment worden deze organisaties binnen de Veiligheidshuizen vertegenwoordigd door pioniers die zeer gemotiveerd zijn om dit concept tot een succes te maken. Wil men echter het concept robuust maken opdat bij verandering van bezetting, of een verschuiving van het aandachtsveld, de formule nog steeds een succes kan blijven, dan zal er een evenwicht moeten worden gezocht tussen de regionale aanpak en een landelijke verankering.

Een ander speerpunt binnen de doorontwikkeling van de Veiligheidshuizen is het nog beter op elkaar laten afstemmen van de preventie en repressie, zorg en strafrechtelijke aanpak. De samenwerking tussen de justitiële keten en de verschillende zorginstellingen kan mogelijk worden uitgebreid om ook voor de (geestelijke) zorgbehoevende doelgroep soelaas te bieden. Daarnaast zijn er ook voorstellen gedaan voor het instellen van een strafrechter die zitting houdt binnen de Veiligheidshuizen in (probleem)wijken. Van deze 'buurtrechter' wordt verwacht dat hij weet wat er in de buurt speelt, waardoor hij direct een 'oorvijg' kan uitdelen

(een gepaste straf kan opleggen) waarvan tevens een preventieve werking uitgaat.

Naast voorgaande voorbeelden, gericht op de toekomst, is er ook een concreet recent voorbeeld te geven. Zo brengt het vraagstuk rond de aansluiting van het Centrum voor Jeugd en Gezin (CJG) op het Veiligheidshuis een specifieke uitdaging met zich mee. Voor een doeltreffende aanpak van gestelde problemen is het noodzakelijk dat de CJG's en de Veiligheidshuizen verbinding hebben en informatie kunnen uitwisselen.
Een CJG opereert slechts preventief en signalerend en doet dit op het terrein van de jeugdzorg. Het Veiligheidshuis opereert daarnaast ook bestuursrechtelijk en strafrechtelijk. Voorkomen moet worden dat op basis van de genoemde functionaliteiten onnodige overlap ontstaat tussen het CJG en het Veiligheidshuis.

Risico's en voorwaarden

Met het specifieke voorbeeld van de te leggen verbinding tussen Centra voor Jeugd en Gezin en de Veiligheidshuizen wordt de focus verlegd van het schetsen van trends naar het bespreken van specifieke risico's. In de 'Uitwerking van de visie op Veiligheidshuizen' (mei 2009) geeft het parket generaal aan dat 'de financiering, het aantonen van effectiviteit en de blijvende bereidheid tot samenwerken van alle betrokken organisaties' als randvoorwaarden worden gesteld voor het succesvol doorontwikkelen van het Veiligheidshuis. Om aan deze randvoorwaarden tegemoet te kunnen komen, zal de focus primair moeten liggen op:

- het voorkomen van nieuwe bureaucratie (coördinatievraagstuk);
- bestendigen van de samenwerkingskaders;
- beperkt houden van de verwevenheid.

Het voorkomen van nieuwe bureaucratie (coördinatievraagstuk)
De trend naar een steeds meer integraal georganiseerde aanpak binnen het Veiligheidshuis draagt automatisch een zeer complex coördinatievraagstuk. Hoe kunnen alle organisaties op één dossier zo efficiënt mogelijk informatie delen en in gezamenlijkheid komen tot één persoonsgerichte aanpak zonder te verzanden in een bureaucratische theekrans. De moederorganisatie (Openbaar Ministerie, politie, Raad voor de Kinderbescherming, reclassering etc.) dient voor het specifieke onderwerp te worden bijgesteld voor deelname aan een Veiligheidshuis. Het gemandateerd acteren binnen een dergelijk samenwerkingsverband bevordert het nakomen en daarmee de uitvoering van gemaakte afspraken. Een verantwoord evenwicht tussen de zaken die per se gezamenlijk dienen te worden aangepakt en onderwerpen die juist binnen het eigen takenpakket vallen, is daarbij noodzakelijk.

Een te grote focus op het idee dat alle problemen binnen het Veiligheidshuis zijn op te lossen, is niet raadzaam. Gevaar schuilt hem daarbij in het uit het oog verliezen van het onderscheid tussen doel en middel. Het Veiligheidshuis blijft immers een middel, een platform voor intensieve samenwerking en afstemming tussen verschillende organisaties. Voorkomen moet worden dat het Veiligheidshuis zich ontwikkelt tot een nieuw bureaucratisch monster waardoor alle voordelen zoals korte lijnen, snelheid en efficiency, samenwerking en onderling vertrouwen in gevaar worden gebracht.

Bestendigen van de samenwerkingskaders
Het evaluatieonderzoek Veiligheidshuizen, dat begin 2009 is uitgevoerd in opdracht van de minister van Justitie, schetst een drietal aandachtspunten voor de toekomst:

- men is onvoldoende gericht op de problemen zelf;
- het ontbreekt aan integrale registratiesystemen en managementinformatie;
- er ontbreken bepaalde partners door onvoldoende vertegenwoordiging, gebrek aan capaciteit of geld en de afhankelijkheid van personen.

Al deze zaken zijn terug te voeren op het onvoldoende vormgeven aan de structuur van de samenwerking (management) tussen de moederorganisatie en het samenwerkingsplatform (Veiligheidshuis). De moederorganisatie (de backoffice) wordt door de netwerkstructuur van het Veiligheidshuis uitgedaagd om vorm te geven aan de rol van de liaison (de frontoffice). De liaison moet immers binnen het Veiligheidshuis de afstemmings-, onderhandelings- en beslissingsbevoegdheid hebben over het handelen van de eigen organisatie om zo de integrale aanpak te kunnen realiseren. Risico hierbij is dat de focus te veel komt te liggen op de identiteit en ontwikkeling van het Veiligheidshuis, waardoor de eigen organisatie aan autoriteit en wellicht ook identiteit moet inboeten.

Samenwerken aan een persoonsgerichte aanpak, door gestructureerd overleg en onderlinge afstemming tussen alle betrokken organisaties, dat is het primaire doel van het Veiligheids-

huis. Om deze essentiële maar tegelijk precaire samenwerking te realiseren en waar mogelijk te borgen, worden allerhande maatregelen getroffen. Een van deze maatregelen is het focussen op lokale initiatieven zonder van bovenaf vaste modellen op te leggen. Alle partners binnen het Veiligheidshuis krijgen de kans om, in overleg met elkaar en afhankelijk van de verschillende betrokken organisaties, een eigen plek te verwerven en samen een werkbare overlegstructuur te realiseren. Toch ontstaat er met de tijd bij met name de grotere nationale organisaties, de behoefte om het beleid richting de veiligheidshuizen te bestendigen en samenwerkingskaders vast te leggen. Het is een uitdaging om te bepalen welke instanties er bij dit vraagstuk moeten worden betrokken en wat hun verantwoordelijkheid is. Het bestendigen van samenwerkingskaders is een belangrijke uitdaging voor het behoud van efficiëntie en effectiviteit binnen het Veiligheidshuis op de lange termijn.

Het beperkt houden van de verwevenheid

Er is een gevoelig spanningsveld tussen enerzijds de steeds verdergaande vervlechting en de mate van autonomie van de individuele organisaties. Samenwerking binnen de publieke dienstverlening kan, mits goed afgestemd, voor een sterk verbeterde effectiviteit zorgen en is derhalve zeer wenselijk. Tegelijkertijd zijn dergelijke samenwerkingsverbanden ook zeer kwetsbaar. Het risico is bijvoorbeeld dat het niet lukt om een structuur te vinden die robuust genoeg is om echte functionaliteit te realiseren binnen het complexe geheel van werkprocessen, afstemmingsvraagstukken en andere uitdagingen. Organisaties hebben naast de taken en verantwoordelijkheden waar zij zich gezamenlijk voor gesteld zien nog tal van andere verantwoordelijkheden binnen het takenpakket, die eveneens hun aandacht vragen.

Vier gouden regels voor de Veiligheidshuis-formule

Zoals uit de voorgaande tekst blijkt, liggen er drie typen uitdagingen voor organisaties die betrokken zijn bij Veiligheidshuizen. Alleen door het Veiligheidshuis 'lean & mean' te houden, kan een nieuwe bureaucratie en daarmee horizontale vervlechting worden voorkomen. De eerste uitdaging betreft het behouden van de probleemgerichte focus bij het werken aan een integrale aanpak over de sectoren straf, zorg en openbare orde en veiligheid. De tweede uitdaging richt zich op het uitbreiden, structureren en bestendigen van de samenwerkingsrelaties tussen partijen op operationeel, management en bestuurlijk niveau, zowel binnen de gemeente als in de regio. De derde uitdaging tot slot richt zich op het beperkt houden van de verwevenheid van individuele organisaties tot wat noodzakelijk is en waarbij op een efficiënte en effectieve wijze wordt samengewerkt.

Onderstaand geven wij vier 'gouden regels' die een leidraad bieden bij het aangaan van deze uitdagingen. Deze regels zijn gebaseerd op opgedane ervaringen binnen Veiligheidshuizen en op de ervaring die Capgemini heeft opgebouwd bij het organiseren van ketensamenwerking in publieke en publiek-private sectoren.

1 Zet het Veiligheidshuis in als gezamenlijke voorziening voor specifieke ketenproblemen
Het Veiligheidshuis is een hulpmiddel in de operationele coördinatie van ketenproblemen op het gebied van onder andere jeugdcriminaliteit, huiselijk geweld, veelplegers, zorg en openbare orde. Aan de basis van ieder casusoverleg binnen het Veiligheidshuis ligt de vraag welk ketenprobleem en daarmee welk coördinatievraagstuk opgelost dient te worden. Alleen die problemen komen in aanmerking, waarvoor géén van de betrokken organisaties alleen of bilateraal een oplossing kan vinden. Alleen als wederzijdse afstemming tussen meerdere partijen noodzakelijk is, heeft casusoverleg en het gezamenlijk plannen en beslissen nut. Dit is daarmee een belangrijk criterium voor de vraag of activiteiten binnen een Veiligheidshuis moeten worden ondergebracht en of dat er aanvullende partijen nodig zijn. Het casusoverleg wordt op basis van het ketenprobleem scherp afgebakend, zowel voor wat betreft de te betrekken organisaties als de personen, casussen of problematiek die besproken worden.

Het Veiligheidshuis zelf kan daarbij gezien worden als een gezamenlijke voorziening die voor een of meerdere coördinatiemechanismen kan worden ingezet. Het Veiligheidshuis vervult een drietal kernfuncties ter ondersteuning van de samenwerking. Om te beginnen als centrale werkplek om het persoonlijk contact tussen professionals uit de betrokken organisaties te faciliteren. Deze kernfunctie bestaat uit het aanbieden van flexplekken, basis-IT-voorzieningen en vergaderfaciliteiten. Ten tweede vervult het Veiligheidshuis een secretariaatsfunctie. Deze secretariaatsfunctie bestaat uit vier onderdelen: 1) het ontvangen van signalen en het agenderen van casussen, 2) het bundelen van actuele informatie van betrokken organisaties tot een integraal persoonsbeeld (casusdossier), 3) de vastlegging van gemaakte afspraken in een behandelplan en 4) monitoring van de voortgang in behandeling. Ten slotte vormt de manager van het Veiligheidshuis de verbindende schakel tussen de 'gebruikers' van de voorziening en is daarmee op tactisch niveau een belangrijke factor voor de intensiteit waarmee wordt samengewerkt. Met deze drie kernfuncties vormt het Veiligheidshuis een aanvulling op de functies binnen de individuele organisaties; alleen bedoeld voor die vraagstukken die ook dit type coördinatie vergen.

2 Richt doelmatige koppelvakken in vanuit de eigen organisatie op het gebied van taken, verantwoordelijkheden en uit te wisselen (informatie)producten
Samenwerkingsverbanden zoals het Veiligheidshuis leggen een claim op de betrokken organisaties ten aanzien van beschikbaarheid van medewerkers, transparantie in informatiepositie en het nakomen van door de organisatievertegenwoordiger gemaakte afspraken. Dit vergt aanpassingen in de interne organisatie. Tegelijkertijd geldt voor de meeste organisaties dat slechts een deel van de zaken via het Veiligheidshuis wordt afgedaan. Het maatwerk dat via de casusoverleggen wordt opgesteld is in beperkte gevallen nodig. Dit geeft een spanningsveld met reguliere taken. Daarnaast geldt voor veel landelijk of regionaal georganiseerde organisaties, zoals in het strafrecht en het OOV-domein, dat de eisen die lokaal worden gesteld ten aanzien van werkprocessen en informatie-uitwisseling op gespannen voet staan met de behoefte aan uniformiteit van processen en efficiënte toepassing van ICT.

Begin met het inrichten van koppelvlakken door een heldere rol en mandaat te definiëren voor de frontofficemedewerkers in het Veiligheidshuis. Hieruit zal ook voor de ketenpartners duidelijk worden wat taken en verantwoordelijkheden zijn. Breng vervolgens het coördinatiemechanisme dat voortvloeit uit deelname in het Veiligheidshuis in balans met andere coördinatie- en prioriteringsmechanismen, zodat de behandeling van zaken en cliënten gelijk en evenwichtig blijft. Ook kan hiermee worden voorkomen dat er frictie ontstaat tussen front- en backoffice, doordat de frontoffice-medewerker toezeggingen doet in het Veiligheidshuis, die niet gedragen en uitgevoerd worden door de achterliggende organisatie.
Vervolgens kan kritisch bekeken worden welke afstemming rondom een casus daadwerkelijk via het Veiligheidshuis moet verlopen. Veel afstemming tussen organisaties behoort tot de reguliere afstemming (bijvoorbeeld het geven van een toezichtopdracht door het Openbaar Ministerie aan de reclassering of de opvolging van overtreding van toezichtvoorwaarden) en vergt geen directe betrokkenheid van een frontoffice-medewerker in het Veiligheidshuis. Wel dient deze persoon uiteraard geïnformeerd te worden als de behandeling van de casus eerder via het Veiligheidshuis verliep.

Ten slotte kunnen werkprocessen en informatie-uitwisseling gestandaardiseerd worden vanuit het perspectief van een backoffice 'in eigen huis' en een frontoffice-medewerker die participeert in casusoverleggen binnen een Veiligheidshuis. Door terug te gaan

naar patronen van samenwerking en informatie-uitwisseling kan worden onderkend welke generieke signalen, casusinformatie en statusberichten gemiddeld genomen nodig zijn ten behoeve van een casusoverleg. Op basis hiervan kan de informatie-uitwisseling (in formulieren en ICT) gestandaardiseerd worden, zodat niet voor ieder Veiligheidshuis een oplossing op maat hoeft te worden ontwikkeld.

3 Laat beleidsmatige sturing op gemeentelijk niveau en in de driehoek
Door de samenwerking in het Veiligheidshuis te concentreren op operationele afstemming over casussen en tactische afstemming over capaciteit, kan de beleidsmatige sturing blijven waar deze hoort: op gemeentelijk niveau en in de driehoek. De gemeente heeft samen met het Openbaar Ministerie een hoofdtaak in het lokale veiligheidsbeleid. De politie faciliteert hierin, evenals andere bij het Veiligheidshuis betrokken organisaties, door het aanleveren van criminaliteitsanalyses. De gemeente stelt het lokale veiligheidsbeleid vast. In die gevallen waar regionale samenwerking een vereiste is, kan dit worden afgehandeld op het niveau van de stadsregio. In het veiligheidsbeleid worden de belangrijkste veiligheidsproblemen geschetst. Vanuit dit lokale beleid is een doorvertaling nodig naar ketenproblemen: waarom heb je welke organisaties nodig om dit probleem aan te pakken. Deze analyse vormt op beleidsmatig niveau de basis voor het afbakenen van doelgroepen en casusoverleggen. De rol van de gemeente is vervolgens die van algemeen opdrachtgever van de partners, die het samenwerkingsverband richting geeft via beleidsnotities, convenanten, subsidies en het monitoren van resultaten in de vorm van hun maatschappelijke effect: metingen. Dit laatste, het evalueren van beleid, vergt enkele afspraken. Om de cohorten te kunnen volgen die via het Veiligheidshuis zijn afgehandeld, dienen betrokken organisaties in hun administratie dit onderscheid te maken. Om de doelmatigheid van de samenwerking te beoordelen, is op het niveau van het Veiligheidshuis inzicht nodig in de mate waarin partijen hun afspraken nakomen.

4 Blijf een faciliterende managementstijl hanteren om de doorontwikkeling een kans te geven
Managers van de betrokken organisaties hebben een scharnierfunctie in Veiligheidshuizen. Ze zijn verantwoordelijk voor inzet van personeel, systemen en middelen. Zij kennen elkaar doorgaans wel, maar anders dan de bestuurders van hun organisaties hebben zij minder groepsbinding. Hun primaire focus is op de eigen organisatie en werkprocessen. Juist de managers kunnen de doorontwikkeling van de Veiligheidshuizen maken of breken. Door het vrijspelen en inzetten van een 'pionier' of juist een 'zorgdrager' kunnen zij sturing geven aan de structurering van de samenwerking binnen het Veiligheidshuis. Dit geldt natuurlijk niet alleen richting de frontoffice-medewerkers die als 'liaison' in het Veiligheidshuis participeren. Het geldt (vooral) ook voor de medewerkers van het Veiligheidshuis, die als regisseur op tactisch en operationeel niveau optreden.

Conclusie

De doorontwikkeling van de vijfenveertig Veiligheidshuizen brengt een aantal uitdagingen met zich mee ten aanzien van probleemgerichtheid, de

rol van het Veiligheidshuis, de bestendiging van de samenwerkingsrelaties en het beperken van bureaucratie en horizontale vervlechting. Door uit het lokale veiligheidsbeleid ketenproblemen te destilleren, krijgt men inzicht tussen welke organisaties coördinatie nodig is bij het aanpakken van specifieke problemen of doelgroepen. Het Veiligheidshuis dient als 'bedrijfsverzamelgebouw' om onderdak te bieden aan de functionarissen die betrokken zijn bij de casusgerichte aanpak. Door de kerntaken van het Veiligheidshuis te beperken tot coördinerende taken als agenderen, bundelen van informatie en monitoren van acties en resultaten, wordt de vervlechting met de betrokken organisaties tot een minimum beperkt. Deze organisaties kunnen op hun beurt het koppelvlak met de veiligheidshuizen uniformeren en faciliteren door standaardisatie van informatieproducten en heldere afbakening van taken en verantwoordelijkheden.

Hiermee kunnen zij een balans aanbrengen in de spanning tussen de frontoffice in het Veiligheidshuis en de backoffice binnen de organisatie. Uitgangspunt is dus het lean & mean houden van het samenwerkingsverband. Dat geldt zeker voor de besturing en de beleidsvorming. Die moeten worden belegd bij gemeente en Openbaar Ministerie en niet leiden tot extra management- of stafvorming binnen het Veiligheidshuis zelf. Doorontwikkeling van de Veiligheidshuizen vergt tenslotte een faciliterende managementstijl vanuit managers van de betrokken organisaties. De huidige samenwerking kent een broos evenwicht dat is opgebouwd uit persoonlijke werkrelaties. Dit vraagt erom dat er vanuit iedere betrokken organisatie zorgvuldig wordt afgewogen welke competenties en persoonlijkheden nodig zijn bij het bestendigen en doorontwikkelen van deze samenwerking. Door de risico's te onderkennen en te focussen op de in dit essay gestelde gouden regels, wordt een bureaucratische theekrans vermeden en kan de Veiligheidshuis-formule tot een doelmatig coördinatieplatform worden doorontwikkeld.

Drs. Dennis van Breemen en drs. Wender van Mansvelt zijn managementconsultants bij Capgemini. Zij zijn gespecialiseerd in juridische beleidsimplementatie binnen de rechtsketen en het onderzoeken van veiligheidsvraagstukken binnen het publieke domein.


BRANDWEER
Ziegler
BL-LV-57

6 Kwaliteitsslag bij de brandweer: waar is de brand?

Leidt formalisering tot een gewenste professionalisering van de dienstverlening?

Drs. Erik Hoorweg MCM
Drs. Roy Schinning

"Een organisatie omvormen die al honderden jaren op dezelfde manier werkt, is op zijn minst een waagstuk te noemen."
Thom de Graaf,
voorzitter Veiligheidsberaad

De brandweer in Nederland heeft momenteel te maken met een van de grootste veranderingen van de afgelopen honderd jaar. Waar voorheen de kwaliteit van de dienstverlening werd afgeleid van de wijze van incidentbestrijding, lijken nu ook andere factoren een rol te gaan spelen. De maatschappij, wet- en regelgeving en onderzoekers stellen steeds verdere eisen aan dienstverlening van de brandweer. Aandacht voor het redden van mensen en bestrijden van incidenten alleen is niet meer voldoende. Van de brandweer wordt verlangd meer in contact te staan met andere dienstverleners, te voldoen aan multidisciplinaire competentie-eisen en het tijdig verlenen van de dienst.

De reactie van de brandweer neigt al snel naar het reorganiseren van de processen en het transparant maken van kwaliteit door middel van geformaliseerde prestatie-indicatoren, keurmerken en certificering (ISO). De vraag die hierbij gesteld moet worden is: leidt deze formalisering wel tot het gewenste effect? Dragen deze wijzigingen nu daadwerkelijk positief bij aan de kwaliteit van de dienstverlening van de brandweer?

Om enig inzicht te geven in structuur, opbouw en dienstverlening van de brandweer is het van belang om een kort beeld te schetsen van 'de brandweer'.

De brandweer in Nederland

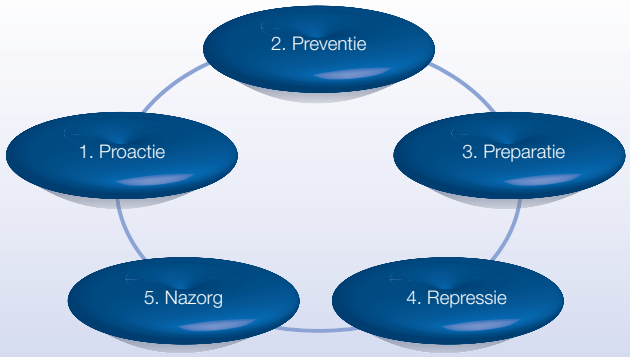
De brandweer in Nederland is op twee niveaus georganiseerd, te weten op gemeentelijk en op regionaal niveau. Nederland kent vijfentwintig brandweerregio's die op termijn allemaal op zullen gaan in vijfentwintig Veiligheidsregio's. Momenteel is het proces van regionalisering gaande, waarbij de gemeentelijke brandweerkorpsen overgaan in de nieuwe vijfentwintig regionale organisaties.

De brandweer is met name bekend als uitvoerder van incidentbestrijding. Het bestrijden van branden, de hulpverlening bij verkeersongevallen en de duiktaak vormen hier onderdeel van. Dit wordt ook wel de repressieve taak van de brandweer genoemd. Bedrijven en instanties met bijzondere risico's zien de brandweer bij controles (van vergunningen) en voorlichting. Dit in het kader van de preventieve taak die de brandweer heeft. De brandweer voert echter meer werkzaamheden uit dan alleen de repressieve en preventietaak.

De kwaliteit van de dienstverlening van de brandweer is met name gericht op het beperken van het effect van een incident.

Ondanks het feit dat de brandweer zich jaren lang heeft toegewijd aan het op peil houden van de kwaliteit van deze dienst lijkt deze niet langer voldoende aan te sluiten bij de wensen en eisen vanuit de maatschappij.

Figuur 1: Beknopte weergave in de vorm van de veiligheidsketen



1. Het voorkomen dan wel wegnemen van structurele oorzaken van fysieke onveiligheid
2. Het voorkomen en beperken van brand
3. Het voorbereiden op een incident
4. Het bestrijden van een incident
5. Het verzorgen van personeel bij verwerken

Trends in maatschappelijke wensen

De brandweer heeft zowel vanuit de wet als vanuit diens maatschappelijke verantwoordelijkheid te maken met een aantal vaste stakeholders. De wensen en invloed van deze stakeholders zijn in de loop der tijd sterk gewijzigd, wat directe gevolgen heeft voor de brandweer in Nederland.

De *bestuurders,* zowel gemeentelijk als op rijksniveau zijn verantwoordelijk voor de bekostiging van de brandweer. Gemeentelijke bestuurders zijn bovendien politiek verantwoordelijk bij een ramp of incident. Bij deze bestuurders bestaat een stijgende behoefte aan meetbare verantwoording van de dienstverlening door de brandweer. Reden hiervoor is de enorme toename van de aandacht voor onderzoeken bij grote rampen of incidenten als de vuurwerkramp in Enschede, de Schiphol-cellenbrand en de vliegtuigcrash van Turkish Airlines. Bij dergelijke incidenten en rampen voeren media en onderzoekers de boventoon. Zodra deze partijen de organisatie van de incidentbestrijding als onvoldoende classificeren, kan dit directe gevolgen hebben voor de verantwoordelijke bestuurders. In het ergste geval leidt dit tot het vertrek van de burgemeester van de betreffende gemeente.[1]

De *bedrijven* en *burgers* zijn feitelijk de klanten van de brandweer. Bedrijven hebben te maken met de brandweer middels preventieve voorschriften en bij incidentbestrijding. Als gevolg van eerder genoemde incidenten is de druk op de brandweer toegenomen waar het gaat om het verlenen, toetsen en adviseren van vergunningen. Denk aan gebruiksvergunningen, bouwaanvragen en milieuvergunningen. De tolerantie voor fouten op dit gebied is kleiner geworden.

Daarnaast lijken burgers minder tevreden over de dienstverlening van de brandweer. Ondanks (of dankzij) het positieve imago van de brandweer,[2] worden de eisen aan tijdigheid, betrouwbaarheid, bekwaamheid hoger. Ook wordt van de brandweer een vergaande klantvriendelijke houding verlangd en dienen de activiteiten van de brandweer voor eenieder uitlegbaar en begrijpelijk te zijn. Dergelijke verwachtingen van burgers zijn terug te zien in de media. Helaas hebben ook brandweerlieden steeds meer te maken met verbaal en fysiek geweld van burgers tijdens de hulpverlening. Of de verwachtingen ten aanzien van de dienstverlening van de brandweer realistisch zijn, is nog maar de vraag. Duidelijk is wel dat de brandweer dient te anticiperen op deze verandering.

Vanuit de *media* is altijd veel aandacht geweest voor brandweer bij rampen en incidenten. Het accent van de berichtgeving lijkt zich echter te hebben verschoven. Stond eerst het uitvoeren van de hulpverleningstaak centraal, nu lijkt het accent meer op de snelheid en accuraatheid van de dienstverlening te liggen. Als voorbeeld kan hierbij gedacht worden aan de brand in het Armando Museum in Amersfoort (2007). In de media was sprake van veelvuldige kritiek op de

[1] Recent voorbeeld hiervan is het vertrek van Fons Hertog als burgemeester van de Haarlemmermeer. Zijn vertrek hing onder meer samen met de Schiphol-brand in 2005.
[2] Conform onderzoek van de Nederlandse Vereniging voor Brandweerzorg en Rampenbestrijding (NVBR).

snelheid van de hulpverlening. Meer in zijn algemeenheid besteden opinieprogramma's uitgebreid aandacht aan resultaten van onderzoeken naar incidenten en de bestrijding hiervan.

Hoe reageert de brandweer op deze hogere maatschappelijke eisen, wensen en verwachtingen?

De vrijblijvendheid voorbij

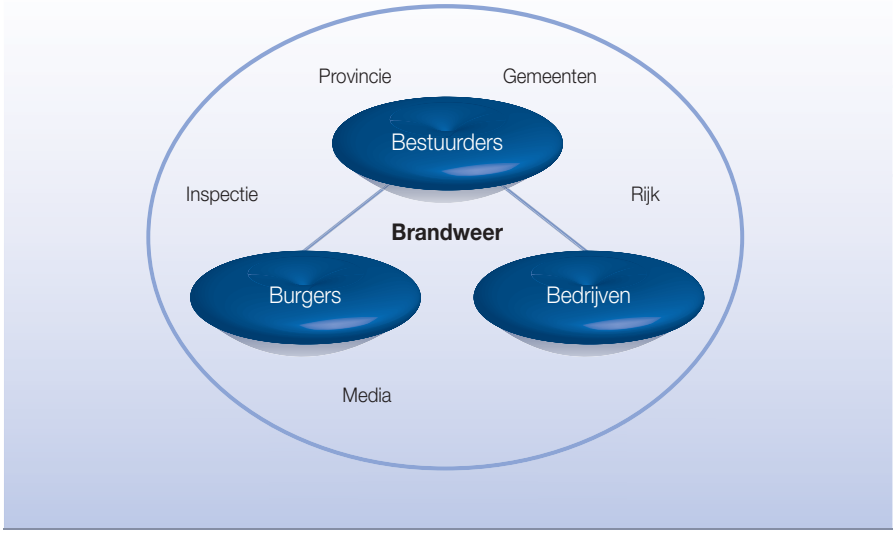
Al deze maatschappelijke ontwikkelingen leiden tot een steeds grotere formalisering van de dienstverlening. Dit vanuit de gedachte dat door transparantie van resultaten een beter gesprek met de stakeholders kan worden gevoerd en hun verwachtingen beter te managen zijn. Het huidige kwaliteitssysteem van de brandweer vindt zijn basis in informele richtlijnen, omschreven in leidraden en handreikingen. Aangezien dit geen formele wetgeving betreft, is het afwijken hiervan juridisch mogelijk.

Nieuwe wet- en regelgeving moet er nu voor zorgen dat die vrijblijvendheid van de richtlijnen tot het verleden gaat behoren. De nieuwe Wet veiligheidsregio's[3] die komend najaar in werking treedt, formaliseert de volgende onderdelen:

- opkomsttijden van brandweervoertuigen;
- competenties van operationele functionarissen;
- bezetting van het eerste voertuig.[4]

Verder kent de wet zodanige kaders dat het in stand houden van een gemeentelijk brandweerkorps bijna onmogelijk wordt. Waar regionalisering voorheen een meer vrijblijvend karakter had, lijkt deze vrijblijvendheid met de komst van de nieuwe Wet veiligheidsregio's voorbij. Doordat kennis en kunde worden samengebracht in één organisatievorm, wordt een impuls gegeven aan de kwaliteit van de brandweer.

Figuur 2: Stakeholders die invloed hebben op de brandweer

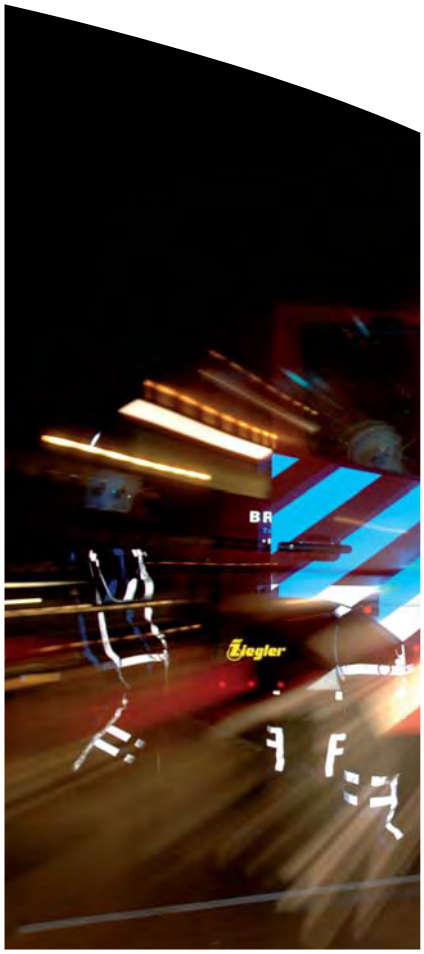


Om de prestaties van onder andere de brandweer meer meetbaar te maken is het project Aristoteles gestart. Dit is een initiatief van de brancheverenigingen van de GHOR en brandweer in samenwerking met het Veiligheidsberaad.[5] Kern van dit project is een uniforme verantwoordingswijze voor alle Veiligheidsregio's.
Hiernaast zijn er initiatieven ontwikkeld vanuit de landelijke brancheverenigingen NVBR om zowel vakinhoudelijk als organisatorisch de brandweerorganisatie kwalitatief op een hoger peil te brengen.
Vakinhoudelijk richt men zich op:

- het verbeteren van het lerend vermogen van de brandweerorganisaties;
- moderniseren van het brandweeronderwijs;
- uniformiteit in informatievoorziening en uitwisseling.

Op strategisch niveau is de brandweer in Nederland gestart met een 'Strategische reis'. In essentie zijn de uitvoeringsverantwoordelijken (regionaal commandanten) van mening dat de huidige brandweer niet langer voldoende aansluit bij de bestaande maatschappelijke inrichting (variërend van complexiteit gebouwen, diversiteit in culturen en technologische vernieu-

[3] Deze wet vervangt onder meer de Brandweerwet 1985. De brandweerorganisatie zal hiermee formeel onderdeel uitmaken van een veiligheidsregio.
[4] Over de beleidsvrijheid van dit onderdeel word nog gedebatteerd.
[5] Het Veiligheidsberaad is een landelijke overlegvorm waarin de voorzitters van de vijfentwintig Veiligheidsregio's zitting hebben.



wingen). Zij achten het noodzakelijk om de focus van de brandweer te verleggen van bestrijding van incidenten naar het voorkomen daarvan. Deze taakverschuiving is bij sommige korpsen reeds te zien aan de komst van projecten op het gebied van Community Safety. Hierbij worden zowel burgers als bedrijven gefaciliteerd in het voorkomen van incidenten in hun eigen omgeving.
Ook in deze 'reis' is de wens uitgesproken om de dienstverlening meer meetbaar te maken. Het doel is om het maatschappelijk rendement van de brandweer inzichtelijk te krijgen. Strengere wetgeving en landelijke initiatieven met bestuurlijk draagvlak zoals hierboven beschreven zorgen ervoor dat het kwaliteitskader van de brandweer steeds formeler van karakter wordt. De vraag is of deze formalisering zal leiden tot de gewenste kwaliteitsslag.

Valkuilen van normering en regulering

Diverse andere publieke dienstverleners, zoals de politie en justitie zijn de brandweer voorgegaan in de formalisering van hun dienstverlening. Daarbij valt op dat na een periode, waarin de hang naar normen en regels de overhand heeft, een nieuwe periode volgt van deregulering en aandacht voor de autonomie en handelingsvrijheid van de professional. Klaarblijkelijk is er sprake van een dialectisch proces. De brandweer kan hier echter nog rekening mee houden en voorkomen dat de normering en regulering te ver doorschiet. Onderstaand zijn enkele valkuilen beschreven:

Prestatiemeting en pervers gedrag
Een bekende reactie op het meetbaar maken van resultaten betreft het eenzijdig aanpassen van het gedrag binnen de betreffende organisatie. Medewerkers, afdelingshoofden, commandanten en/of directeuren zijn geneigd om zich in te zetten op die onderwerpen die ook in de sturingsinstrumenten zijn geoperationaliseerd in prestatieindicatoren. Een bekend voorbeeld binnen een andere overheidssector betreft prestatieindicator 'snelheidsovertredingen' bij de politie. Een deel van het budget werd aan de korpsen toegekend op basis van deze indicator. Dit heeft de eerste jaren na introductie van deze indicator geleid tot de zogenaamde 'flutzaken'. Dit zijn zaken die wel bijdragen aan de bekostiging van een korps, maar weinig tot niets toevoegen aan de maatschappelijke veiligheid. Los daarvan heeft de sturing op outputindicatoren geleid tot een nadruk op de repressieve kant van politiewerk. Met preventieve inspanningen op het gebied van bijvoorbeeld huiselijk geweld of advies inbraakpreventie snijdt de politie zich (paradoxaal genoeg) in de vingers. Dit betekent immers minder aangiften en daarmee minder 'productie'. Ook bij de zittende magistratuur (rechtbanken) heeft een dergelijke ontwikkeling plaatsgevonden. Nadat rond het jaar 2000 met het programma Lamicie de outputnormen voor de afhandeling van zaaksaantallen was doorgevoerd, is in de navolgende jaren een vrij eenzijdige nadruk op productie komen te liggen. Na circa vijf jaar zijn echter weer nieuwe initiatieven ontstaan om de kwaliteit van het werk te verbeteren.

Causaliteit of plausibiliteit?
Een tweede valkuil betreft de vermeende causaliteit tussen de input (mensen, middelen en budget) via throughput tot output. Met de introductie van en sturing op indicatoren wordt ervan

uitgegaan dat een inzet van een bepaalde hoeveelheid mensen, middelen en budget op een bepaalde wijze zal leiden tot het gewenste resultaat (output). De toets of dit resultaat ook echt volledig is te beïnvloeden door de betreffende organisatie wordt echter vaak vergeten. Niet voor niets wordt er momenteel veel gediscussieerd over de normen voor de opkomsttijden. Daarnaast is het de vraag wat output-indicatoren betekenen voor de eerder genoemde stakeholders. Burgers en bedrijven zijn vooral gebaat bij het uiteindelijke effect van de preventieve en repressieve inspanningen. Dan gaat het om minder incidenten, minder schade, minder doden en gewonden en betere bestrijding. Met andere woorden, dan gaat het om outcome of maatschappelijk effect. Meting van dit effect vraagt om ex post evaluatie-onderzoek in plaats van periodieke meting van volledig beïnvloedbare prestaties.

Normering versus professionalisering

Vaak wordt normering en regulering gezien als een middel om een organisatie te professionaliseren. Normen en de daarbij behorende meetinstrumenten maken processen en resultaten transparant en daar kan men van leren. Dit kan inderdaad het geval zijn. Echter, deze meetinstrumenten worden vaak vooral gebruikt om elkaar aan te spreken of af te rekenen. Het lerend effect van normering beperkt zich dan tot enkelslag leren. Echte professionalisering geschiedt via opleiding en training.

Opleiding raakt de kern van dienstverlening

De brandweer staat voor een enorme uitdaging. Na vierhonderd jaar optimaliseren van het proces 'water naar vuur brengen' heeft de brandweer met zijn Strategische Reis een geheel nieuw model voor ogen. Het continuïteitsconcept en focus op maatschappelijk rendement vragen om een ander soort kwaliteit dan met regels en normen kan worden afgedwongen. Regels en normen geven aan hoe de organisatieleden zich dienen te gedragen en te handelen. Het zegt niets over het waarom en waartoe.

Met het oog op de beoogde ontwikkeling binnen de brandweer zou de discussie zich moeten richten op de onderliggende opvattingen en principes binnen de organisatie. Hierbij gaat het om de inzichten en basiswaarden van de brandweerlieden. Deze gedeelde inzichten en basiswaarden worden in de opleiding meegegeven. De brandweer kent een hechte en duidelijk eigen cultuur. Men kan op elkaar rekenen, ook in levensbedreigende situaties. Het is juist deze sterke onderlinge verbondenheid die een goede basis vormt voor de beoogde kwaliteitsverbetering. Door aanpassing van het opleidingsprogramma en investeringen in bijscholing kan kwaliteitsverbetering worden doorgevoerd in lijn met de Strategische Reis en vanuit het hart van de brandweer. Formalisering van de dienstverlening door regulering, prestatie-indicatoren en normering biedt op z'n best inzicht en een basis voor dialoog met stakeholders.
Echter, de valkuilen van pervers gedrag, windowdressing en afrekenen liggen daarbij op de loer!

De sleutel van de echte kwaliteitsverbetering zit in het sturen van de basiswaarden van de brandweer binnen de opleiding.

Drs. Erik Hoorweg MCM en drs. Roy Schinning zijn managementconsultants bij Capgemini. Erik Hoorweg richt zich op besturing en beheersingsvraagstukken, organisatiedoorlichting en intelligence binnen het veiligheidsdomein.
Roy Schinning richt zich op regionaliseringvraagstukken en is gespecialiseerd in de brandweer en Veiligheidsregio's.


Pizzeria
STAR MEUBEL

7 Beheerst u integrale veiligheid in uw organisatie?

Integrale veiligheid door beheersing van veiligheidsrisico's.

Drs. Roeland de Koning
Ron Massink

Veiligheidsrisico's

Van oudsher heeft een organisatie te maken met safetyrisico's, gerelateerd aan ongelukken, arbo-zaken (aantasting van werknemersgezondheid) en milieubelasting (vervuiling van de omgeving). Daarnaast zijn de risico's voor de informatievoorziening de laatste jaren steeds belangrijker geworden (waardevolle informatie). Steeds vaker krijgen organisaties te maken met criminaliteit die interne schade veroorzaakt en de bedrijfsvoering verstoort, variërend van diefstal (van laptops uit kantoorgebouwen), tot bedreigingen van medewerkers, geweldsdelicten tegen personeel, bedrijfsspionage en acties van bijvoorbeeld dierenrechtenactivisten.

Dit soort toevallige en/of moedwillige aantasting van de organisatie is met name een te managen aspect in de bedrijfsvoering voor organisaties die actief zijn in het beheer van kritische infrastructuur zoals betalingsverkeer, (kern)energievoorziening, drinkwaterproductie, transportknooppunten.
Ook organisaties die specifieke waardevolle en of controversiële processen uitvoeren (onderzoek en ontwikkeling) of waardevolle producten produceren (waardepapieren, olie en gas) zijn een kwetsbare groep.
Security staat bij dit type organisaties al enkele jaren separaat op de agenda, naast de zorg voor safety, arbo en milieu. Dit creëert een versnipperde aanpak van risicomanagement, versnipperde aandacht van het management en suboptimale maatregelen om risico's te verkleinen. Integrale veiligheid is in veel organisaties nog in het begin van haar ontwikkeling.
Dat biedt kansen voor de functionele manager om de veiligheidsfunctie naar een hoger niveau te brengen. Kansen in de zin van kostenreductie, schaalvoordelen, bewust risico's accepteren en een positieve veiligheidsbeleving in de organisatie.
In dit hoofdstuk beschrijven wij een visie op de integratie van de beheersing van veiligheidsrisico's, die de assets (alles wat van waarde is) van een organisatie schade kunnen berokkenen. Dit hoofdstuk beschrijft een aanpak en toekomstbeeld van de ontwikkeling van integrale veiligheid.

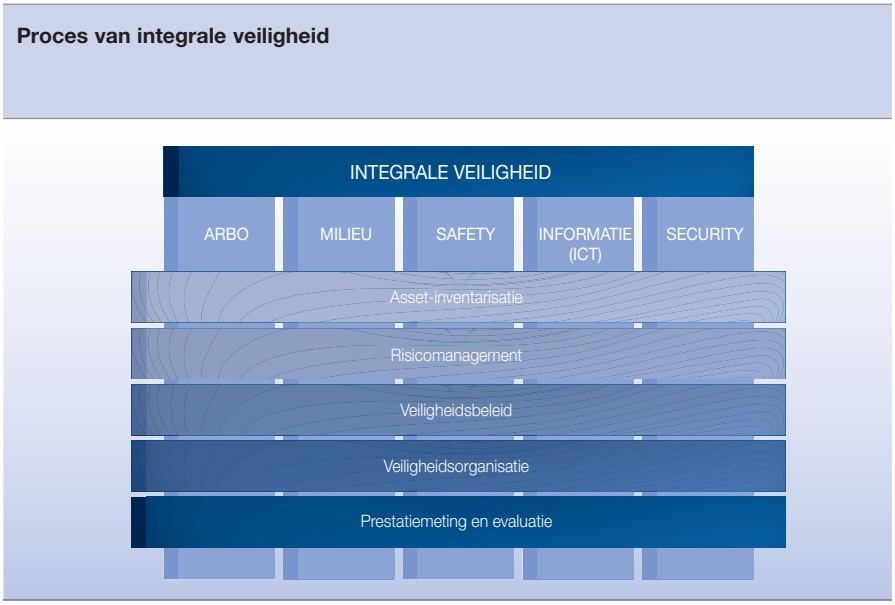
Integrale veiligheid

Er bestaat momenteel geen regelgeving op het vlak van integrale veiligheid. Separaat is er wetgeving op safety-, arbo- en milieuvlak, afhankelijk van de sector is er regelgeving op het vlak van security. Na een aansprekend incident is er vanuit de publieke opinie steeds vaker de roep om beheersing van risico's. Accepteren van risico's en daaruit voortvloeiende acceptatie van schade is moeilijk verkoopbaar. Het grote publiek verwacht dat een organisatie op alle aspecten van veiligheid haar bedrijfsvoering op orde heeft.
Vaak zien we dat door één specifiek incident en door emotie, die met dat incident gepaard gaat, de effectiviteit van de maatregelen en de beheersing van kosten buiten proporties zijn voor de organisatie. Wij zijn van mening dat door een integrale benadering van veiligheid

- minder kosten gemaakt worden;
- een positieve veiligheidsbeleving binnen de organisatie ontstaat;
- schaalvoordelen worden bereikt;
- bewust risico's worden geaccepteerd, waardoor de marktpositie van de organisatie verbetert.

Bij integrale veiligheid wordt gekeken naar statische risico's, zoals de risico's

Proces van integrale veiligheid



die voortvloeien vanuit safety, security, informatie, arbo en milieu. Bij integrale veiligheid wordt dus niet gekeken, zoals bij 'enterprise riskmanagement', naar alle risico's die de continuïteit van een organisatie bedreigen. Bij integrale veiligheid wordt niet gekeken naar de zogenaamde dynamische risico's: politieke risico's (wetgeving), economische risico's (conjunctuur), financiële risico's (beurs), juridische risico's (aansprakelijkheid). Veiligheidsincidenten tasten de continuïteit van de organisatie aan, terwijl die juist gegarandeerd dient te worden. Het gaat dus om de vraag 'Hoe bescherm ik wat van 'waarde' is voor mijn organisatie?' Daarbij kan men denken aan financiële waarde, maar ook aan maatschappelijke waarde(n), het effect op het welzijn van medewerkers en burgers, de omgeving en het imago van de organisatie.

In de praktijk wordt veiligheid veelal versnipperd opgepakt. Er is in veel organisaties een aparte afdeling die verantwoordelijk is voor arbo, een aparte functionaris voor milieuzorg en een team met mensen actief met informatiebeveiliging. Dat is op zich nog niet zorgelijk. Het feit dat al deze afzonderlijke disciplines eigen methoden en technieken hebben om te bepalen waar het grootste risico zit en wat de juiste maatregelen zijn om die risico's te verkleinen, is dat wel. Want het gevolg daarvan is dat het geheel van statische risico's niet op een eenduidige wijze wordt bestuurd. Is het risico van een arbo-incident groter dan een risico van een een safety-incident? Moet ik meer investeren in het voorkomen van milieuschade of meer maatregelen nemen tegen informatiediefstal?
Het ontbreekt bij het management aan overzicht ten aanzien van veiligheidsrisico's die zijn organisatie loopt. Vanuit de verschillende functionele afdelingen worden op zich effectieve, preventieve maatregelen (technische, organisatorische, personele maatregelen) voorgesteld. Er zijn vaak allerhande activiteiten op het gebied van veiligheid, maar de verbinding tussen deze activiteiten ontbreekt. Door deze gefragmenteerde aanpak en gebrek aan integrale verantwoordelijkheid heeft het management van de organisatie geen overzicht en is daarmee niet in control over zijn veiligheidsrisico's. Naast het vraagstuk van efficiëntie en doelmatigheid, onderwerpen die in een tijd van economische crisis zeker niet onbelangrijk zijn, is het tevens van belang om veiligheid mee te nemen bij strategische beslissingen. Waar zet ik mijn nieuwe fabriek neer? Welke risico's kleven er aan de productie van mijn nieuwe product? Wil ik onderzoek gaan doen met behulp van dierproeven? Welke structurele veiligheidseisen stel ik aan de bouw van een nieuw winkelcentrum? Om antwoord te geven op deze strategische vragen en keuzes te maken op tactisch/operationeel niveau is het wenselijk om een procesmatige aanpak te hanteren voor de beheersing van veiligheid.

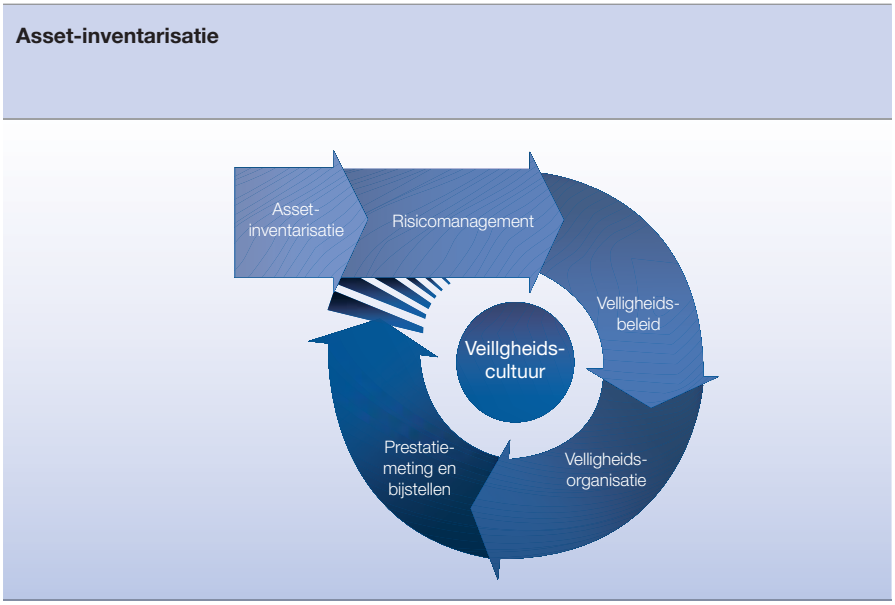
Integrale veiligheid

Integrale veiligheid is een procesmatige aanpak om grip te krijgen op alle statische veiligheidsrisico's en om weloverwogen mitigerende maatregelen te nemen. Maatregelen die aansluiten op de bedrijfsprocessen en deze niet belemmeren. Dit proces is een geïntegreerde, risicogeoriënteerde benadering met een gestructureerde, systematische kijk op de veiligheid van de organisatie. Hierdoor is de organisatie permanent voorbereid op aantasting van de waardevolle bedrijfsprocessen en wordt tegelijkertijd de waarde van de assets beschermd. Integrale veiligheid is een thema dat de kern van de bedrijfsvoering raakt en dat niet enkel een safety-, security-, ICT-, arbo- of

milieuvraagstuk is. Het streeft daarbij naar het in stand houden van de functionele expertisegebieden, met de borging van een aantal uniforme processen.

Met integrale veiligheid is de organisatie in staat om een checklist op te leveren die een bestuurder elke morgen maximaal vijf minuten bekijkt. Die bestuurder kan noodzakelijke risico's verantwoord nemen, onzekerheid beïnvloeden en verantwoordelijkheid dragen. Om dit te kunnen doen, moet de organisatie volwassen zijn in haar beheersing van veiligheid.
Het integraal managen van alle statische risico's binnen een organisatie zonder integrale veiligheidsfuncties is een moeilijke opgave. Het is erg lastig om alle functioneel verantwoordelijken gelijkertijd in één 'ruimte' een gezamenlijk besluit te laten nemen. Een andere uitdaging is het voorkomen van begripsverwarring ten aanzien van het begrip risico (risico's die bij het dagelijks werk horen versus risico's die duidelijk met gevaren (hazard) te maken hebben). Daarnaast is een gelijk detailleringsniveau van risico's en maatregelen noodzakelijk om deze onderling te vergelijken.
Om te komen tot integrale veiligheid zijn de volgende aspecten van belang: asset-inventarisatie, risicomanagement, veiligheidsbeleid, veiligheidsorganisatie, prestatiemeting en -bijstelling en cultuur (veiligheidsbewustzijn).

Asset-inventarisatie
Startpunt van integrale veiligheid is het zicht hebben op de waardevolle 'assets' in de organisatie (veiligheidsobjecten). Wat zijn zaken van 'waarde' voor de organisatie? Dit kunnen zowel fysieke zaken zijn, als immateriële zaken als personen in of imago van de organisatie.

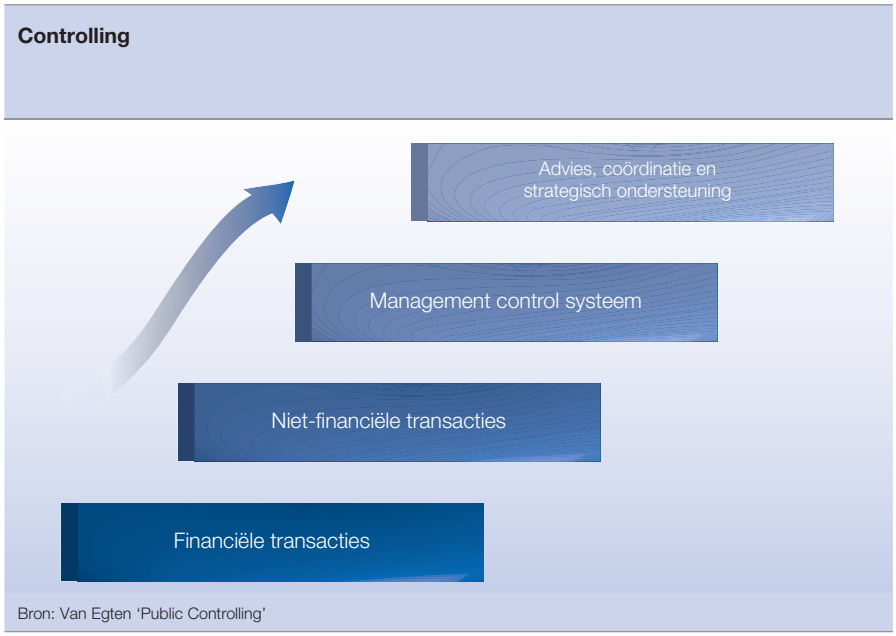


Risicomanagement
Relevante risicoscenario's worden opgesteld voor de onderkende veiligheidsobjecten en beoordeeld door scores toe te wijzen op impact en voorstelbaarheid. Hiermee wordt een risicoprofiel voor de organisatie geschetst dat input is voor het veiligheidsbeleid.

Veiligheidsbeleid
Op basis van de vastgestelde risico's dient een beleid geformuleerd te worden hoe met deze risico's om te gaan. Keuzes worden gemaakt voor het accepteren dan wel mitigeren van deze risico's. In het beleid worden verantwoordelijkheden voor veiligheid benoemd, alsook de uitgangspunten voor de technische, bouwkundige en organisatorische maatregelen.

Veiligheidsorganisatie
De veiligheidsorganisatie vormt het hart van integrale veiligheid aangezien in dit onderdeel van het proces de maatregelen daadwerkelijk worden uitgevoerd. De veiligheidsorganisatie is met name functioneel verantwoordelijk voor het proces, maar heeft ook de bevoegdheid daarop in te grijpen. Door het overzicht dat deze organisatie heeft, is dit daarvoor de meest geëigende positie. De verantwoordelijkheid voor veiligheid binnen onderdelen van de organisatie op zich blijft een lijnbevoegdheid. Daaronder vallen de feitelijke maatregelen, instructies en het integreren van het thema veiligheid in gedragscodes. De vastlegging van deze maatregelen in plannen en procedures vormt een sluitstuk op de set aan maatregelen.

Prestatiemeting en -bijstelling
De effectiviteit van de veiligheidsmaatregelen is het uiteindelijke doel van alle inspanningen. Dan is het ook goed om regelmatig te meten of de huidige set aan maatregelen voldoet. Door het vooraf bepalen van prestatie-indicatoren wordt een raamwerk geboden voor het toetsen van de werking. De resultaten uit metingen vormen input voor het bijstellen van de



Bron: Van Egten 'Public Controlling'

bestaande opzet en zijn daarmee instrumenten in een continu proces van kwaliteitsverbetering.

Cultuur: veiligheidsbewustzijn
Veiligheid effectief binnen organisaties implementeren is gebaseerd op een breed draagvlak en individueel eigenaarschap op het thema. Dat betekent dat er niet een persoon of afdeling is die zich met veiligheid bezighoudt, maar dat iedereen verantwoordelijk is voor zijn persoonlijke werk/leefomgeving en daar als eigenaar over waakt. Enkel een slot op een deur hebben is niet voldoende, de deur mag dan ook niet open blijven staan. Het gedrag van medewerkers is bepalend of een organisatie daadwerkelijk veilig is. Een bewustwordingstraject is nodig om medewerkers bewust te maken van de veiligheidsrisico's en om deze medewerkers te informeren wat zij zelf kunnen doen.

De toekomst van integrale veiligheid in de bedrijfsvoering

Bovenstaand proces van integrale veiligheid is een ideaal beeld. Dit ideaal beeld is niet van de een op andere dag bereikt. Als we kijken naar andere functies in de bedrijfsvoering zien we dat deze functies door de jaren een groei hebben doorgemaakt.

De ontwikkeling van integrale veiligheid als volwassen bedrijfsonderdeel heeft overeenkomsten met de groei van de controllersfunctie. Prof. Van Egten schetst in haar boek 'De controlfunctie in de publieke sector' de groei van de controlfunctie in een organisatie. In de jaren '50 startte de controlfunctie met het beheersen van financiële transacties. Later kwamen daar ook niet-financiële transacties bij. Om overzicht te houden, ontwikkelt de functie zich nu naar het beheren van een managementcontrolsysteem dat instrumenten bevat zoals risicoanalyses, begrotingen, forecast-rapportages, audits en doorlichtingen. Wanneer de controller deze instrumenten bezit, is hij in staat om een dominante informatiepositie op te bouwen en op basis daarvan strategisch advies te geven aan de top, ten behoeve van besluitvorming.

Ook integrale veiligheid zal als bedrijfsfunctie naar die positie moeten groeien, zodat er op basis van een informatiepositie advies gegeven kan worden ten behoeve van besluitvorming. Voor integrale veiligheid zal een stap gemaakt moeten worden van het functioneel gescheiden monitoren en beheersen van veiligheidsissues naar het integraal monitoren en beheersen van alle statische veiligheidsissues.

Integrale veiligheid vraagt om het doorlopen van een stapsgewijze ontwikkeling. Naar analogie met het INK-model zijn er vijf fasen te onderscheiden in de 'volwassenheid' van de organisatie. Het INK-model is algemeen bekend in de wereld van bedrijfsvoering. Het geeft een eenvoudig ontwikkelpad voor de beheersing van het kwaliteitsvraagstuk in een organisatie. Het managen van integrale veiligheid is in essentie het streven naar kwaliteitsverbetering. De volwassenheid van integrale veiligheid kan dan ook geanalyseerd worden naar analogie van de INK-ontwikkelfasen.

Een korte toelichting op de fasen, vertaald naar de veiligheidsfunctie:

Fase 1 Activiteit-georiënteerd
De functionele afdeling kan voor een groot deel zelf bepalen wat zij doet. Op haar eigen manier streeft de afdeling ernaar het werk zo goed mogelijk uit te voeren.

Het afdelingsbeleid kan worden getypeerd als ad hoc en korte termijn, er is geen gezamenlijke opvatting over de inhoud en vormgeving van veiligheidsmaatregelen. Problemen krijgen pas aandacht als er incidenten zijn.

Fase 2 Proces-georiënteerd
Het proces wordt beheerst en de processen zijn geïdentificeerd binnen de functionele afdeling. Taken, verantwoordelijkheden en bevoegdheden van de professionals zijn helder geformuleerd. Afspraken zijn vastgelegd. Verbeteringen binnen de processen vinden plaats op basis van geconstateerde afwijkingen.

Fase 3 Systeem-georiënteerd
Er wordt systematisch gewerkt aan de verbetering van de individuele functie. De plan-do-check-act cyclus wordt toegepast. De afdeling wil proberen incidenten te voorkomen in plaats van te verhelpen. Het beleid heeft draagvlak binnen de afdeling en wordt goed uitgedragen door de leiding van de afdeling.

Fase 4 Keten-georiënteerd
De doelmatigheid en doelgerichtheid van de afdeling worden bevorderd door deze af te stemmen met andere afdelingen. Men onderhoudt contacten, werkt samen, houdt rekening met wensen van andere afdelingen en vergelijkt de eigen prestaties met die van andere afdelingen.
Per afdeling wordt bepaald wie het meest geschikt is om een bepaalde taak uit te voeren. Besturingssystemen worden met elkaar verbonden. Innovatie staat voorop.

Fase 5 Integrale veiligheid
Integratie van processen tussen functi onele afdelingen/functies met behoud van eigen expertise. Het proces van continu verbeteren is in de structuur en de cultuur verankerd. Op basis van een langetermijnvisie worden tijdig de bakens verzet; de organisatie loopt voorop met nieuwe ontwikkelingen. Op basis van deze modellen kan de veiligheidsfunctie binnen een organisatie worden geanalyseerd en kan beoordeeld worden waar de verbeterpunten liggen op het vlak van integrale veiligheid. Door te leren van de ontwikkelingen die de controlfunctie en de kwaliteitsfunctie hebben doorgemaakt binnen het domein van bedrijfsvoering, kunnen we bovendien een voorspelling geven van de positie van integrale veiligheid in de organisatie.

Integrale veiligheid staat in veel organisaties nog in het begin van haar ontwikkeling. Dat biedt kansen voor de functionele manager om de veiligheidsfunctie naar volwassenheid te brengen. Kansen in de zin van kostenreductie, schaalvoordelen, bewust risico's accepteren en een positieve veiligheidsbeleving in de organisatie. Wat is uw volwassenheidsniveau op het vlak van integrale veiligheid? Steeds vaker zal het management keuzes moeten maken, die de functionele domeinen van veiligheid doorkruisen of beïnvloeden. Ook goede externe verantwoording dwingt de organisatie tot een gecoördineerde aanpak van veiligheid. Beheerst u de statische veiligheidsrisico's in uw organisatie?

Kwaliteit: INK ontwikkelingsfase

Bron: INK-model

Drs. Roeland W.J. de Koning is managementconsultant bij Capgemini en gespecialiseerd in de veiligheidssector. Hij is gespecialiseerd in risicomanagement en security-management.
Ron Massink is manager Integrale Veiligheid bij de TU Delft, CEO van Lindyn Risicomanagement en partner bij Tripple S Hazard Risk Management. Hij is gespecialiseerd in de integratie van veiligheids-/riskmanagement bij organisatiedoelen, alsmede ontwerp van veiligheids- en crisismanagement-instrumenten.

8 Beter functioneren door in anderen te investeren

Drs.ing. Erik van den Berg
Mr. Patrick de Graaf

Netcentrisch werken betekent oogsten door te investeren, zowel bij de initiële invoering ervan, als in de dagelijkse operatie. Hoe de balans te vinden tussen halen en brengen, tussen investeren en oogsten?

'Ontvrienden' is een begrip dat u en wij nog niet kenden aan het begin van 2009. Er bleek een nieuw begrip nodig te zijn om een nieuwe trend te duiden. In de loop van 2009 zijn veel mensen tot het inzicht gekomen dat er iets niet klopt aan het hebben van meer dan duizend vrienden op sociale netwerksites als Hyves of Facebook. Ze zijn massaal gaan ontvrienden. Zo massaal dat dit begrip het woord van het jaar 2009 is geworden. Via dit nieuwe woord hebben we nu ook zicht op de tegengestelde trend van 'ontvrienden', namelijk die van het opbouwen van omvangrijke sociale netwerken via het web.

Iets vergelijkbaars is er aan de hand bij de informatievoorziening voor veiligheid. Het verbeteren van de eigen informatiepositie door gebruik te maken van de informatie van anderen, is inmiddels breed in de praktijk verankerd. Gelukkig maar. Is het bijvoorbeeld nodig om precies te weten wat er in het brandende binnenvaartschip zit, achterhaal dan de partij die hier iets van weet en haal daar de benodigde informatie. De tegengestelde trend, namelijk zelf actief informatie inbrengen als partij met cruciale informatie voor betere hulpverlening of crisisbestrijding, staat nog in de kinderschoenen. 'Halen' en 'brengen', beide zijn nodig voor verhoging van de effectiviteit van operatie en besluitvorming, wanneer het er echt om gaat. 'Netcentrisch werken' is het toverwoord.

In dit hoofdstuk doen we een pleidooi voor het opschalen van netcentrisch werken, voor halen en brengen. We zien dat dit echter niet vanzelf gaat en geven daarom ook enkele handreikingen om organisaties te helpen, die verder willen met netcentrisch werken.

Wat is netcentrisch werken?

Netcentrisch werken heeft als concept flink bestuurlijk terrein gewonnen in het domein van incidentmanagement, rampenbestrijding en crisisbeheersing. Wat is het eigenlijk? Netcentrisch werken is een operationeel concept, waarin besluitvormers, informatieleveranciers en eenheden in een geïntegreerd interactief informatienetwerk samenwerken. Dus bijvoorbeeld de informatie van de politieagent ter plaatse wordt aan gegevens uit basisregistraties van de gemeente toegevoegd en gedeeld met allen. Van minister tot burgermeester tot brandweerman.
Het idee is dat beter en sneller delen van informatie in zo'n netwerk van actoren leidt tot betere besluiten en betere inzet van mensen en hulpmiddelen. De effectiviteit van het geheel neemt daardoor toe. De spil van de informatievoorziening is het gedeeld actueel operationeel beeld. Iedereen heeft dezelfde actuele informatie. Het gaat om informatie over bijvoorbeeld het incident zelf, slachtoffers, omgevingsfactoren (bijvoorbeeld meteo) en de organisatie van de hulpverlening. Het totaalbeeld is opgebouwd uit informatie van de verschillende spelers. Hierdoor verbetert voor elke speler de informatiepositie. Het gemeentelijk Centraal Registratie en Informatiebureau houdt bijvoorbeeld een registratie van slachtoffers bij en de brandweer geeft gegevens door uit

metingen naar emissies van gevaarlijke stoffen.
Netcentrisch werken is afgeleid van de militaire concepten Network Centric Warfare en Networked Enabled Capabilities. Ook hierbij staat een gedeelde situational awareness centraal. Iedere militair of (mechanische) sensor (radar, infrarood etc.) geeft actief informatie door om aan bevriende partijen een zo compleet mogelijk beeld te geven. Alle deelnemende entiteiten profiteren daarvan, wat de slagkracht en overlevingskans van eenieder én het geheel drastisch vergroot. Digitale informatie-uitwisseling is voor de strijdkrachten van vandaag een essentieel onderdeel van de operatie en besluitvorming.

Vertaling naar samenwerking in veiligheidsregio's

Het netcentrische concept spreekt aan in veiligheidsland. Uit oefeningen en evaluaties van echte rampen blijkt namelijk telkens dat een goede informatievoorziening gebaat is bij het tijdig en juist delen van informatie met iedere direct betrokken partij. De eigen, interne informatievoorziening op orde hebben is niet voldoende. Anderen hebben ook gegevens nodig, alleen weet je niet altijd wie wat precies wanneer nodig heeft. De veelheid aan crisissituaties die zich kan voordoen, maakt een complete voorbereiding ondoenlijk. Je moet daarom meer flexibiliteit inbouwen in de informatievoorziening.

Nederland is onderverdeeld in vijfentwintig veiligheidsregio's waar, binnen de kaders van de Wet veiligheidsregio's, wordt samengewerkt door besturen en diensten ten bate van brandweerzorg, rampenbeheersing, crisisbeheersing, Geneeskundige Hulpverlening bij Ongevallen en Rampen (GHOR) en de handhaving van de openbare orde en veiligheid. Om aan de hoge eisen van deze wet te voldoen, zullen de Veiligheidsregio's netcentrisch werken wel moeten doorvoeren. Het Veiligheidsberaad heeft dan ook de invoering van netcentrisch werken tot een van zijn prioriteiten benoemd.[1] Het doel is alle betrokken bestuurders en hulpverleners in realtime over een eenduidig beeld van incident, ramp of crisis te laten beschikken.
Veel veiligheidsregio's boeken momenteel al aanzienlijk vooruitgang bij de implementatie van het netcentrisch werken. Dit geldt zeker voor de veiligheidsregio's waar brandweer en GHOR een gezamenlijk veiligheidsbureau hebben en een multidisciplinaire informatiemanagementfunctie is ingericht. Een goed en noodzakelijk begin. Ook voor deze regio's zijn echter nog moeilijkheden te overwinnen. Denkt u bijvoorbeeld aan informatiedeling met andere actoren zoals de politie, gemeenten, waterschappen, defensie, vakdepartementen en overige rijkspartners, private partijen, buurregio's en instanties in buurlanden. Nu heeft bijvoorbeeld de buurregio die assistentie verleent niet dezelfde informatiepositie als de regio waarin het incident plaats heeft.

Op zoek naar balans

Zoals uit de beschrijving van netcentrisch werken blijkt, gaat het niet alleen om gebruiken, maar ook om verstrekken van informatie. Het is

[1] Naast het versterken van functioneren meldkamers, onderhoud en vernieuwing C2000 en aansluiting op de basisregistraties. Zie: http://www.veiligheidsberaad.nl/smartsite.

echter voor de verstrekker niet altijd duidelijk of hij daar zelf (direct) bij gebaat is. Waarom tijd en geld steken in het weggeven van gegevens? Voor een organisatie is het niet vanzelfsprekend om opvragen en (proactief) verstrekken van informatie met elkaar in balans te brengen.
Het 'halen' van informatie uit de omgeving is nog altijd kenmerkend voor de meeste publieke en private organisaties met een veiligheidstaak. Vanuit het eigen perspectief kan dat heel logisch en rationeel zijn. Je moet immers een afweging maken in de inzet van schaarse middelen. Wat is op lokaal niveau de kans dat er zich een dermate grootschalig incident voordoet, waarvoor netcentrisch werken nodig is? Het is verleidelijk nog maar even te wachten met de noodzakelijke investering…

Naast de rationele argumenten op basis van tijd en geld, spelen er ook andere argumenten om nog maar even niet over te gaan tot netcentrisch werken. Zo bestaat er soms weerstand tegen het 'zo maar' delen van informatie met anderen. Wat doet die ander ermee? Wie gaan er nog meer met die informatie aan de haal? Zijn anderen wel deskundig genoeg om deze informatie te beoordelen? Is het wel veilig? Ben ik nog wel belangrijk genoeg als mijn informatie overal beschikbaar is?

Daarnaast ontbreekt naast geld en tijd vaak ook kennis om bijvoorbeeld informatiesystemen te koppelen met andere, of zelfs te vervangen. De gebruikers zijn bovendien vaak gehecht aan het eigen systeem en de mogelijkheden ervan. Dit soort argumenten kunnen het delen van informatie of koppeling van informatiesystemen in de weg staan.[2]

Pragmatische oplossingen werken, echter…

Om volledig te kunnen profiteren van het netcentrisch gedachtegoed is het nodig de informatie-uitwisseling fundamenteel anders te organiseren.
Op weg naar netcentrisch werken is een aantal praktische oplossingen voorhanden om informatie te delen:

Fysiek in dezelfde ruimte werken
Samenwerking en onderlinge afstemming worden sterk verbeterd als partijen op dezelfde locatie werken. Zo is er bijvoorbeeld het veiligheidsbureau, waar de GHOR en brandweer hetzelfde gebouw delen. Zij delen vaak ook de meldkamer. Tijdens een inzet delen de GHOR, brandweer en politie vaak dezelfde motorkap in het 'motorkapoverleg'. Ook in een beleidsteam komen de kopstukken van alle betrokken organisaties fysiek samen voor overleg.

Echter…
Hoe partijen te informeren die niet op dezelfde locatie aanwezig zijn, is minder goed geregeld. Zij kunnen vaak na afloop van het overleg pas vernemen wat er aan de hand is en wat er dient te gebeuren. Dit kan minuten tot uren later zijn. Situatie en informatie zijn dan vaak al weer achterhaald.

Onderling afstemmen via bijvoorbeeld telefoon of C2000
Naast systemen als C2000 zijn de mobiele telefoon, mobilofoon of marifoon veelgebruikte hulpmiddelen. 'We kennen elkaar goed en we bellen dan even met elkaar.' Deze werkwijze leidt tot snelle en directe afstemming.

Echter…
Hoe partijen die niet gebeld worden of niet in dezelfde (C2000)-gesprekgroep zitten, worden geïnformeerd, is wel een probleem. Het aantal mensen dat je kunt bellen of door wie je gebeld kunt worden tijdens ramp of crisis is beperkt. Zeker als je tegelijkertijd de hulpverlening moet organiseren. Behoor je niet tot de gelukkigen die de leidinggevende te spreken kan krijgen via telefoon of C2000, dan blijf je verstookt van eventuele cruciale informatie. We hebben het dan nog maar even niet over beperkingen in de capaciteit van het netwerk.

De meldkamer als informatieknooppunt
De meldkamer is goed, altijd en makkelijk te bereiken voor zowel hulpdiensten als door burgers. De meldkamer krijgt zeer veel meldingen en andere informatie te verwerken, stuurt operationele diensten aan en legt onderlinge verbanden. Wie moet waar zijn om wat te doen? De meldkamer reikt operationele hulpdiensten de essentiële informatie aan om snel en goed te kunnen handelen. De meldkamer is een cruciaal knooppunt voor informatie en coördinatie.

Echter…
De meldkamer is geoptimaliseerd op de intake van informatie en de snelle verwerking daarvan. De meldkamer is er echter niet op toegerust om, buiten de operationele C2000-verbindingen om, informatie door te geven. Partijen die niet betrokken zijn bij de eerste en

[2] http://www.binnenlandsbestuur.nl/default.lynkx?tag=tcm:25-1082514

urgente hulpverlening worden momenteel niet of nauwelijks geïnformeerd vanuit de meldkamer. Een informatieknooppunt wordt volgens ons dan al snel een informatieput. Informatie stroomt er naartoe, maar er eenmaal in, niet meer uit.
Pragmatische oplossingen werken, maar laten nog grote gaten liggen in de informatievoorziening. Fnuikend voor effectief optreden in geval van nood. We moeten het netcentrisch werken daarom op grote schaal doorzetten.

Bevorderen van netcentrisch werken

Op basis van een visie op langere termijn kan netcentrisch informatie delen geleidelijk worden gerealiseerd. Welke stappen kunnen vrijwel direct worden gezet onderweg naar netcentrisch werken? We noemen hieronder een aantal belangrijke zaken, zonder overigens uitputtend te willen zijn.

- Investeer in de relatie. Leer elkaar kennen en probeer begrip te krijgen voor elkaars verantwoordelijkheden tijdens incident, ramp of crisis. Ken ook de eigen beperkingen en heb oog voor de synergie die door samenwerking kan ontstaan.
- Bedenk wat je voor een ander kunt doen (waarvan je zelf in ieder geval niet minder wordt), met name in de zin van informatie delen. Maak in het verlengde daarvan bestuurlijk afspraken over informatieleveringen. Stel hiervoor ook een leveringsovereenkomst op, die concreet aangeeft welke informatie je op welke basis en voorwaarden zal leveren aan de afnemende partij, waarmee de overeenkomst is aangegaan. Zo weet iedereen waarvoor hij staat voor levering van informatiediensten (als publicist) en wat iedereen kan verwachten aan informatiedienstverlening (als afnemer).
- Maak informatieverspreiding en samenwerking tot expliciete en belegde verantwoordelijkheden binnen de eigen organisatie. Neem het op in de eigen planvorming en begroting en oefen de uitvoering daarvan.
- Gebruik gezamenlijke uitgangspunten voor de informatievoorziening om samenwerking tussen alle partijen te bevorderen. Zie bijvoorbeeld de uitgave 'Het informatiebeleid Veiligheid: verbinding in veiligheid'.[3] Het gaat dan bijvoorbeeld om gedeelde doelen (goedkoper, robuuster etc.), maar ook inhoudelijke handvatten. Naast netcentrisch werken zijn dat (onder andere) de Informatiearchitectuur Sector Veiligheid (IASV) en de Architectuur Informatiebeleid Veiligheid (A-IBV). Meer informatie hierover is te verkrijgen bij het informele landelijke overleg OOV-architecten.[4]
- Gebruik gemeenschappelijke voorzieningen waar die er zijn, in plaats van eigen voorzieningen in te richten of een woud aan externe koppelingen aan te leggen. Denkt u bijvoorbeeld aan basisregistraties of geografisch materiaal (kaarten). De baten van het gebruik van gemeenschappelijke voorzieningen liggen niet alleen in de informatie die dit oplevert, maar ook in besparingen op koppelvlakken of het beheer van eigen voorzieningen (inclusief bijvoorbeeld licentiekosten).

[3] Op te vragen, evenals het gehele manifest Principes informatiebeleid veiligheid via informatiebeleidveiligheid@minbzk.nl. Zie ook http://www.minbzk.nl/actueel?popup=t...&ActItml dt=117068.
[4] Te bereiken via looovarchitecten@vtspn.nl

- Als een externe koppeling van het eigen informatiesysteem met andere systemen toch nodig is, gebruik dan de beschikbare standaarden en een gemeenschappelijke taal. De eerder genoemde IASV is hierbij behulpzaam.

Netcentrisch werken vraagt van overheden een haast Von Münchhausen-achtig vermogen om zichzelf op een hoger plan te tillen. Zijn er nog externe krachten om jezelf uit het moeras te trekken?

Publiek-private samenwerking als hulpmiddel

In het bedrijfsleven is de afgelopen decennia veel knowhow opgebouwd over met name de operationele kant van netcentrisch werken en informatiedeling in het algemeen. Zo zouden we nog steeds geen voertuigposities met elkaar kunnen delen als het bedrijfsleven dit niet zou hebben gefaciliteerd met landelijke voertuigpositieservers voor zowel de brandweer als de ambulances. Een ander voorbeeld is het Programma Ladinggegevens, waarin publieke en private leveranciers van informatie (zoals de Rotterdamse haven) een verkeersplein voor informatie hebben ingericht. We zien dat het ministerie van BZK inschakeling van het private innovatievermogen ook steeds meer beschouwt als hulpmiddel voor praktische inbedding voor het Informatiebeleid Veiligheid.[5]

Wat zijn grondslagen van goede publiek-private samenwerking tegen de achtergrond van het doel om goede gemeenschappelijke voorzieningen voor de sector veiligheid binnen nu en vijf jaar te hebben gerealiseerd? We richten ons hier óók op (en tot) de private kant van de zaak.

- Het begint met het delen van een visie, een hoger doel dat partijen ook op kritieke momenten bij elkaar houdt. Om de ambities waar te maken zijn groot uithoudingsvermogen en vastberadenheid nodig. Een gedeelde visie steunt dit.
- Eigen financiering, niet te veel, niet te weinig. Zowel te weinig als te veel geld leidt tot niets. Grote ICT-budgetten staan zelden voor evenredig grote resultaten. Het kan ook efficiënter. Bedrijven die zelfstandig (voor)investeren, moeten dat doen met een budget dat een factor kleiner is dan van een vergelijkbaar overheidsprogramma. Dit noopt tot creativiteit, veel oog voor hergebruik en voor partnerships met partijen die iets sneller, beter of goedkoper kunnen dan de eigen organisatie. De creativiteit zal niet alleen in ontwerp of techniek tot uiting moeten komen, maar ook in het financieringsmodel en het governancemodel.
- Bereid zijn risico's (over) te nemen. Steeds meer overheden én bedrijven gaan gebukt onder een cultuur van risicomijdendheid. Overheden zijn al te vaak door de media of politieke partijen op het publieke hakblok gelegd. Managers van bedrijven worden beloond op het kortetermijnresultaat. Investeringen die pas na een jaar of meer gaan renderen zijn daarom voor menig manager een no-go. Binnen bedrijven is ondernemerschap nodig, het liefst concreet gemaakt in een investeringsbudget. Echter, een ondernemer stapt ook pas ergens in als hij zelf zeker weet dat er vraag is naar zijn product of dienst. Daar waar er geen betalende klanten in het vizier zijn, stopt hij.
- Transparant aanbod. In alles wat je levert of belooft, wees transparant. Wat gaat het kosten? Wat krijg je nu en wat is er mogelijk over een jaar. Hoe is de beheerorganisatie ingeregeld? Hoe ziet het governancemodel eruit? Wat is het niveau van beveiliging? Dit soort vragen moeten helder te beantwoorden en verifieerbaar zijn, wil er vertrouwen kunnen zijn in de publiek-private dienst die aan het ontstaan is.

Eerst eens vrienden worden

Het wordt wel eens grappenderwijs gezegd: "Om te kunnen vermenigvuldigen, moet je eerst leren delen." Dat geldt voor netcentrisch werken als concept zeker, maar ook voor totstandkoming van deze wijze van werken. We moeten de slag maken van 'halen' naar 'brengen én halen'. Iedereen die bijdraagt aan het effectiever en efficiënter maken van incidentmanagement, rampenbestrijding of crisisbeheersing kan daar zijn voordeel mee doen en zo bijdragen aan een veiliger samenleving. Voordat we aan ontvrienden toekomen, zullen we eerst maar eens meer vrienden moeten maken.

Drs.ing. Erik van den Berg en mr. Patrick de Graaf zijn consultants bij Capgemini.
Erik van den Berg is gespecialiseerd in de informatiearchitectuur van de sector Veiligheid.
Patrick de Graaf richt zich op strategie en innovatie van IT-organisaties in en voor de publieke sector.

[5] http://digitaalbestuur.nl/opinie/veiligheid-bij-bzk


A.U.B. armen houden
zoals afgebeeld.
3 sec.
Please, raise arms
according to picture.

9 De grens voorbij

Drs. Nico Kaptein
Jule Hintzbergen

De landsgrenzen zijn onlosmakelijk verbonden met de identiteit van een staat en zijn inwoners. De overheid besteedt veel aandacht aan grensbewaking, vooral om te bepalen wie en wat het land in of uit mag. De staat bewaakt op deze wijze de veiligheid, reguleert de economie en beïnvloedt de sociale ontwikkelingen.

We leven in een tijd waarin het internet, Europese samenwerking en internationaal zakendoen vanzelfsprekend zijn geworden. Een tijd waarin de reisbewegingen van mensen nog elk jaar toenemen, waarin mensen gewend zijn aan comfort. De overheid dient haar rolopvatting als grensbewaker aan deze ontwikkelingen aan te passen. Reizigers, vliegvelden en luchtvaartmaatschappijen accepteren geen urenlange wachttijden meer. Tegelijk willen mensen veilig kunnen vliegen, zonder dat iemand een bom in zijn boxershort kan verstoppen. Ook willen we voorkomen dat de verkeerde mensen ons land binnenkomen en voorkomen dat bezoekers er onoorbare praktijken op nahouden zoals mensenhandel, terrorisme of andere georganiseerde criminaliteit.

Wereldwijd zoeken overheden naar de juiste balans tussen gemak en veiligheid aan de grens. Hierbij spelen vragen als: welke risico's willen we managen en op welke wijze handhaven we de wetten en regels? Naast nationaalpolitieke afwegingen spelen ook internationale verplichtingen en afspraken een belangrijke rol. In dit essay betogen we dat enerzijds technologie alleen de grenzen niet veiliger zal maken, terwijl anderzijds veiligheid en privacy niet tegenover elkaar hoeven te worden geplaatst. Het wordt tijd wereldwijd minder reactief op dreigingen te reageren en op een verstandige manier gebruik te maken van de beschikbare kennis en middelen.

De grens beslaat in een moderne definitie niet alleen het geografische punt van overgang van het grondgebied van de ene en de andere staat, maar omvat ook administratieve en logistieke knooppunten in de landen van herkomst en bestemming. Het besluit om mensen en goederen al dan niet toe te laten op de fysieke grens kent een aantal besluitvoorbereidende stappen. Hierin spelen informatievergaring en de wil en het vermogen om informatie te delen een belangrijke rol. Hoe beter de grensbewaker geïnformeerd is, hoe hoger de kwaliteit van zijn besluit. Dit vraagt om een actieve overheid, die haar ketens op orde heeft. Effectief en efficiënt samenwerken tussen de diverse overheidsinstanties in Nederland en ook daarbuiten, is een randvoorwaarde voor een adequate grensbewaking.
Kortom, in Nederland wordt de grensbewaking gebruikt voor het managen van meerdere risico's.

De grensbewaker kan besluiten tot een interventie op basis van signalen en informatie. Terwijl de aard van deze signalen en informatie zeer divers is, ligt de uiteindelijke oorsprong altijd bij de mens die sporen achterlaat. Een veilige grenspassage gaat uiteindelijk altijd over mensen, niet over dingen. Hoewel er veel aandacht uitgaat naar goederen, bagage en transportmiddelen leert de ervaring dat risico's en veiligheid uiteindelijk altijd zijn terug te voeren tot personen. Tegenwoordig zijn er methoden en technieken om op basis van de persoonlijke achtergrond en het vertoonde gedrag van individuen een behoor-

lijke analyse te maken van de risico's om iets of iemand over de landsgrens te vervoeren. Hierbij wordt onder andere gebruikgemaakt van profielen. Als een jonge vrouw vanuit een bepaald land inreist in gezelschap van een oudere man, dan weten we hoe we kunnen onderzoeken of er sprake kan zijn van mensensmokkel of gedwongen prostitutie. Bagage die niet of niet duidelijk tot een meereizende persoon is terug te voeren, kan in beginsel een aanwijzing zijn dat er iets mee aan de hand is. Op basis van dergelijke inzichten zijn al veel maatregelen genomen.

Deze methoden en technieken worden ook gebruikt om criminaliteit en terrorisme te bestrijden, waarbij de grens fungeert als een willekeurig controlepunt. Voor het plegen van aanslagen kan het nodig zijn (dat denken sommige verantwoordelijke autoriteiten in ieder geval) om cruciale onderdelen of stoffen het land in te voeren.

Belangrijk is ook de financiële invalshoek. Met bijvoorbeeld 'carrouselfraude' wordt de grens gebruikt om de nationale autoriteiten een rad voor ogen te draaien en meer belasting terug te krijgen dan wordt betaald. Ook is gebleken dat criminaliteit en terrorisme goed bestreden kunnen worden door de geldstromen te volgen en/of te blokkeren. Op financieel gebied hebben onze overheden een achterstand opgelopen op de criminaliteit.

Met goede afspraken, wet- en regelgeving en operationele samenwerking en het benutten van gegevens, die allang worden verzameld, kan veel worden bereikt met bestaande kennis en kunde. Cyber crime verdient aparte aandacht (zie ook de bijdrage van Patrick de Graaf en Mike Tettero): volgens schattingen is 80% van de schade die wordt veroorzaakt door georganiseerde criminaliteit gerelateerd aan cyber crime. Dit staat in schril contrast met de wijze waarop we met dit onderwerp omgaan. Ook in de bovenwereld valt er nog wel wat op te lossen. Waar wordt belasting betaald over internettransacties? Kortom, aan de slag zou je zeggen: we begrijpen de problematiek, kunnen beschikken over heel veel gegevens en als we deze maar goed bijeenrapen en analyseren, weten we precies hoe we het beste kunnen interveniëren. En o ja, laten we, als we hebben gezien dat het werkt, ook nog iets doen aan de privacy en zorgen dat we op zijn minst kunnen uitleggen dat we behoorlijk voldoen aan alle wet- en regelgeving. Toch?

Deze aanpak is riskant. Een werkwijze als in de VS, waarin het doel alle middelen heiligt, is in strijd met essentiële waarden in onze samenleving. Denk hierbij aan Guantanomo Bay, aan mensen persoonlijk tot terrorist of misdadiger bestempelen op basis van algemene risicoprofielen. Het is ook niet nodig om een dergelijke richting in te slaan, omdat er inmiddels oplossingen zijn om binnen de context van onze waarden en regels de gewenste effecten te bereiken, mits hiermee van aanvang af rekening wordt gehouden.

Om zo zeker mogelijk te weten wie je voor je hebt, kun je gebruikmaken van zogenoemde biometrische gegevens - gegevens die betrekking hebben op unieke lichaamskenmerken, zoals de structuur van de iris, het patroon van een handpalm, een vingerafdruk. Ook geautomatiseerde gezichtsherkenning is biometrie. In de praktijk wordt bij gebruik van dergelijke gegevens veelal een groot bestand aangelegd waar ook allerlei andere gegevens over personen worden opgeslagen. Riskant, zeker omdat als dergelijke biometrische gegevens 'op straat' komen te liggen er niet altijd een reparatie mogelijk is. We hebben maar tien vingers, dus als de vingerafdrukken niet meer bruikbaar zijn… Er zijn allerlei oplossingen (niet onnodig allerlei gegevens opslaan, encryptie gebruiken, gegevens niet centraal opslaan maar gecompartimenteerd etc.), maar deze worden zelden goed toegepast. Om bijvoorbeeld met biometrie te onderbouwen dat degene die heeft ingecheckt dezelfde persoon is als degene die aan boord van een

vliegtuig stapt, is het voldoende om een biometrisch gegeven te registeren en vervolgens te valideren. Er hoeven geen andere persoonlijke gegevens te worden opgeslagen. Toch is het nog geen gemeengoed om in een dergelijk geval zo'n mate van soberheid in het opslaan van gegevens te betrachten. Bovendien kunnen vanwege geldende wetgeving biometrische gegevens niet zo maar tussen publieke en private organisaties worden uitgewisseld.

Nog een voorbeeld: steeds meer wordt gebruikgemaakt van passagierslijsten, met name op luchthavens, om inkomende vluchten vooraf te onderzoeken op inzittenden waarvoor de autoriteiten een meer dan gemiddelde belangstelling hebben. Vaak worden gegevens eenvoudig verzameld en gekoppeld aan allerlei politiegegevens. Verzuimd wordt nogal eens goed na te denken over welke gegevens nu echt nodig zijn, en wie er toegang toe dient te hebben. Dit leidt ertoe dat of er vanwege privacy en wetgeving veel gegevens worden afgesloten van het analyseproces, dan wel dat onnodig veel mensen toegang hebben tot gegevens die in beginsel iemand in gevaar of in verlegenheid kunnen brengen. Ook hier: er zijn oplossingen op de markt om privacy en veiligheid veel nauwkeuriger te combineren. In sommige landen (zoals ook Nederland) worden gegevens overigens alleen bewaard en gekoppeld als er een match is gevonden, dat wil zeggen wanneer een passagier voldoet aan een risicoprofiel of persoonlijk wordt gezocht. Alle andere gegevens worden conform EU-regelgeving binnen 24 uur weer verwijderd.

Het komt nogal eens voor dat in het kader van grensmanagement lichtzinnig voor technologische oplossingen wordt gekozen, zonder dat het onderliggende probleem goed is geanalyseerd en een proces is bedacht om met het probleem om te gaan. Waarom zijn zo ongeveer alle luchthavens wereldwijd ertoe overgegaan om bodyscanners te bestellen in de eerste weken na de mislukte aanslag in Detroit (december 2009)? Meer dan een Pavlov-reactie op de media-aandacht en de publieke opinie is het niet. Zelfs al kan het scannen van mensen en goederen een goede bijdrage leveren aan onze veiligheid, dan niet overhaast en ondoordacht. De kosten die hiermee gemoeid zijn, zijn astronomisch hoog. Om wereldwijd het risico te minimaliseren, kunnen twee miljard reizigers worden gecontroleerd met scanners die miljarden kosten, los van de extra tijd die dit gaat kosten, terwijl men nog maar moet afwachten of er werkelijk mensen op deze manier tegen de lamp gaan lopen. Deze kosten moeten uiteindelijk door de goedwillende reiziger worden betaald. De 'echte' terrorist of crimineel zal zijn doel toch bereiken, omdat maar al te vaak vergeten wordt dat technologie te omzeilen is en een aanvulling moet zijn op mensenwerk.

En wie heeft het drieregelige bericht gezien waaruit bleek dat in april 2010 de Europese overheden hebben afgesproken dat per 2013 weer flesjes aan boord van vliegtuigen meegenomen mogen worden? Waarom kon het eerst niet en nu toch? Of was het allemaal wat kortzichtig en overdreven?

Het is beter te investeren in het op verantwoorde wijze verbeteren van de intelligence-functie en de onderlinge samenwerking tussen organisaties en mensen.

In Nederland loopt het programma Vernieuwing grensmanagement, onder leiding van de IND en de Koninklijke Marechaussee. De timing is prima: net nu de Nederlandse overheid de moeite neemt het gehele proces en de informatievoorziening daar omheen eens goed onder de loep te nemen, en nog wel in samenhang, zijn zowel de inzichten en middelen beschikbaar om dat op een moderne, verantwoorde manier te doen.
Technologie alleen is nooit een oplossing, we moeten er wel bij blijven nadenken. Het is ook al lang niet meer nodig om privacy en veiligheid tegenover elkaar te zetten. Het gaat al met al niet meer om technologische mogelijkheden of beperkingen, het gaat om het maken van een fundamentele keuze op basis van een visie en strategie gebaseerd op onze democratische normen en waarden.

Ons pleidooi is om, uitgaande van een visie op informatiegestuurd optreden, naast technologie ook privacy op de agenda te plaatsen. En meer dan angst en mediahypes, juist de opbrengst van investeringen mee te wegen en nooit te vergeten dat grensmanagement mensenwerk is: samenwerkende mensen en organisaties maken met elkaar onze wereld veilig en leefbaar.

Drs. Nico Kaptein is als principal consultant bij Capgemini werkzaam als vakgroepleider Public Security en director of Operations Public Security binnen de global Public Sector.
Jule Hintzbergen is managing consultant Public Security bij Capgemini en gespecialiseerd in intelligence, biometrie en ketensamenwerking.


RONOS
906
906
Verboden toegang
voor onbevoegden

10 Europa, sta op en maak de wereld veiliger!

Drs. Nico Kaptein

Het lukt in Europa niet om de regie over openbare orde en veiligheid in eigen hand te houden. Hoewel de beste ideeën uit Europa lijken te komen, zijn de Verenigde Staten zoveel meer daadkrachtig en eenduidig in hun optreden, dat zij de facto bepalen hoe het internationale veiligheidsbeleid zich ontwikkelt. Schrijnend is dat in Europa binnen en tussen de verschillende lidstaten in veel gevallen inhoudelijk in grote mate overeenstemming bestaat over de te volgen koers. Deze koers wijkt echter af van het beleid van de VS en uiteindelijk komen de Europese plannen te laat om de Amerikaanse richting nog wezenlijk te beïnvloeden. Het Verdrag van Lissabon biedt nieuwe kansen.

Een voorbeeld: in de Rotterdamse haven wordt hard gewerkt aan '100% containerscanning'. Het klinkt goed: als je alles scant, vind je alles en voorkomen we aanslagen en smokkel. Echter, wie even doordenkt, begrijpt dat hier sprake is van een schijnveiligheid. Door de schaarse middelen evenredig te verdelen over alle containers die langskomen, is er maar weinig tijd en aandacht voor de afzonderlijke containers. We weten overigens hoe het wel moet: doe een risicoanalyse en selecteer de nader te onderzoeken containers op basis van kennis en analyse van eerdere ervaringen met betrokken bedrijven en personen en een analyse van het transport op basis van ontwikkelde profielen. Op deze wijze worden middelen optimaal ingezet om risicovolle transporten nader te onderzoeken.

Let wel: deskundigen en overheden zijn het binnen Europa eens: 100% controles hebben in het algemeen geen zin en vergroten de onveiligheid. Toch laten we ons in een situatie brengen waarin het logisch lijkt in het kader van internationale samenwerking en economische belangen het beleid van de VS over te nemen.

Nog een voorbeeld: in de meest recente nieuwjaarsnacht vloog ik van Bonaire naar Amsterdam. Kort na het opstijgen werd door de bemanning van het vliegtuig gemeld dat 'op last van de Amerikaanse overheid' het flight trackingsysteem was uitgeschakeld. Dat was waar ook: een week eerder was een Nigeriaan na een vlucht van Lagos via Amsterdam naar Detroit door een medepassagier in de kraag gegrepen bij een mislukte poging in het vliegtuig - kort voor de landing - een ontploffing te veroorzaken. Blijkbaar was de assumptie dat als je geen flight trackingsysteem hebt, je niet weet wanneer je er bijna bent en zeker geen aanslag kunt plegen. Navraag leerde dat een nieuwe maatregel was uitgevaardigd, dat vliegtuigen boven Amerikaans grondgebied of water geen flight tracking mogen tonen aan passagiers. Een maand later is de hele maatregel alweer ingetrokken - ook de VS hebben ingezien dat het probleem wel eens ergens anders gevonden zou moeten kunnen worden - hadden we dat niet zelf kunnen bedenken?

Een ander hoogtepunt vond een paar maanden eerder plaats op een vlucht van Amsterdam naar Washington, waar 'op last van de Amerikaanse overheid' het samenscholen met meer dan twee personen bij de toiletten was verboden… Hoe komt het toch dat er nooit iets te horen is als: 'op last van de Europese Commissie'? En waarom accepteren we met elkaar dergelijke, weinig betekenisvolle maatregelen klakkeloos?

De Europese Unie is nog steeds aan het herstellen van 9/11: sinds 2009 durven we onze democratische waarden weer gelijk te stellen aan het belang van veiligheid. Kijk de nieuwe Europese onderzoeksagenda er maar eens op na. Eén keer per jaar organiseert het land dat op dat moment de EU voorzit een conferentie om de innovatieagenda voor openbare orde en veiligheid voor de komende jaren te presenteren en te bespreken. Deze conferentie is een belangrijke graadmeter voor de stand van het denken in Europa. Het resultaat is afgestemd met vertegenwoordigers van lidstaten van de EU, zelfs besproken met enkele niet-leden die constructief meedenken (zoals Israël en Zwitserland) en geeft een goed beeld van waar we het met elkaar over eens zijn.
Vol trots is het afgelopen jaar in Stockholm op deze conferentie aangekondigd dat we de Europese waarden weer belangrijk vinden. We doen er al een kleine tien jaar over om de impact van de aanslagen in New York en Washington van ons af te schudden en onze eigen identiteit en ideeën over de wereld weer centraal te stellen in ons denken. Op zich wrang dat we dit 'innovatie' noemen. En waar is onze identiteit de afgelopen tien jaar gebleven? Democratie is in Europese ogen toch echt wat anders dan wat Amerikanen 'freedom' noemen. Hoelang zou het gaan duren voordat we de hernieuwde basis ook in gezamenlijk beleid en uitvoering hebben omgezet?

Inhoudelijk vinden Amerikaanse en Europese overheden de problematiek net zo lastig: het volk roept om snelle en zichtbare maatregelen. Het is klaarblijkelijk moeilijk om onder deze druk even de tijd te nemen om eerst op basis van een grondige analyse het beste plan te kiezen, en dit vervolgens ook op een effectieve manier uit te voeren. En het kan zo maar zijn dat de investeringen langer doorgaan dan het kortetermijngeheugen van de media reikt, terwijl de effecten later zichtbaar worden, of alleen voor ingewijden. Het kost nu eenmaal tijd om inlichtingendiensten beter samen te laten werken, meer tijd dan het kost om deze in naam onder één noemer te plaatsen. Het Department of Homeland Security werkt echt niet effectiever dan voorheen de verschillende diensten deden, die in de organisatie zijn opgegaan. Na de mislukte aanslag bij de landing in Detroit tijdens de kerstdagen van 2009 leek de reactie van Obama verdacht veel op die van Bush na 9/11. Kortom, laten we in Europa met elkaar beleid ontwikkelen en vooral principes en uitgangspunten vaststellen. En daar dan ook aan vasthouden als het spannend wordt.

Het leuke is dat in de relatie met de Aziatische wereld de verhoudingen evenwichtiger lijken. Een goed voorbeeld is de samenwerking met Chinese autoriteiten en havenorganisaties om de controle in de transportketen in samenhang te laten verlopen. Loopt dit nu anders omdat onze filosofie meer op de Chinese lijkt, of omdat we ons als Europa anders hebben opgesteld? Het lijkt erop dat een rol speelt dat dit grotendeels tussen landen onderling kon worden geregeld. Toch heeft ook de Europese regelgeving geholpen, waarbinnen in toenemende mate ruimte wordt geschapen voor andersoortige controlemechanismen, gedeeltelijk gebaseerd op vertrouwen naast controle. Veel meer in lijn met de eerder besproken filosofie om juist te controleren waar het nodig is.

Met het Verdrag van Lissabon dat recentelijk van kracht is geworden, heeft Europa enorm aan kracht gewonnen. Bijna niemand heeft het in de gaten, zo lijkt het, maar de slagvaardigheid van de Europese Commissie en ook van bijvoorbeeld Europol, is enorm toegenomen. Waar tot voor kort besluiten alleen unaniem konden worden genomen, is nu een gekwalificeerde meerderheid voldoende.

Waarom is dit zo belangrijk? In Europees verband wordt stevig vergaderd. Doorgaans doet de Commissie op de dag dat een onderwerp inhoudelijk wordt behandeld ter plekke een tekstvoorstel dat voor een deel van de aanwezigen op dat moment nieuw is. Tot dusverre kon een lidstaat die niet ter plekke een standpunt kon of wilde innemen een 'voorbehoud' maken. In de praktijk betekende dit één of twee maanden vertraging voordat kon worden doorgepraat of besloten.

Anno 2010 kan dit niet meer. Het voorbehoud betekent niets, want ook met een stem minder kan een besluit gewoon worden genomen. Lidstaten moeten zich nu anders voorbereiden en afgevaardigden worden gemandateerd om ter plekke hun inbreng te leveren en een standpunt in te nemen.

Al met al zijn er serieuze kansen om het heft weer in handen te nemen. De verschuivende machtsverhoudingen in de wereld maken het nodig niet langer alléén naar de Verenigde Staten te kijken. En ook binnen de VS zijn de verhoudingen verschoven, zodat de impact van een gemoderniseerde Europese opstelling ook voor de VS hanteerbaar zal blijken.
Een helder eigen geluid maakt het mogelijk vol in te zetten op internationale samenwerking zonder mee te deinen op de golven, die worden veroorzaakt door krachten buiten Europa. Overheden en bedrijven zoeken in toenemende mate internationale samenwerking. Het huidige Europese beleidsvacuüm remt de energie en innovatie onnodig af.

We zijn het aan de wereld verplicht op dit punt beter samen te werken en voor onze inzichten op te komen. En wie kunnen binnen Europa het voortouw beter nemen dan wij Nederlanders? Met of zonder VOC-mentaliteit kunnen we Europa helpen mede richting te geven op weg naar een veiligheid binnen de kaders die we daarvoor met elkaar willen stellen.

Drs. Nico Kaptein is als principal consultant bij Capgemini werkzaam als vakgroepleider Public Security en director of Operations Public Security binnen de global Public Sector.

Thoughtleadership Capgemini

Rechts treft u twee andere interessante rapporten aan.
Voor een compleet overzicht van ons thoughtleader gedachtegoed zie www.capgemini.nl

Daar geven onze markt- en IT-experts hun visie op variërende onderwerpen in trendsrapporten, onderzoeken en white papers.

Navigerend transformeren in publieke organisaties

Overheidsorganisaties staan onder druk om te veranderen. Publiek en politiek willen efficiënte en snelle oplossingen voor tal van maatschappelijke problemen op gebieden zoals jeugdzorg en integratie. Een succesvol antwoord ligt buiten de eigen organisatiegrenzen, buiten de eigen kolom en buiten het eigen beleidsterrein of de eigen keten. Het boek is het resultaat van onderzoek en gesprekken met topambtenaren, bestuurders en managers van publieke organisaties, uitgevoerd door Capgemini Consulting. De vraag die centraal staat: hoe kun je als publieke organisatie zodanig transformeren dat je betere dienstverlening kunt bieden, tegen lagere kosten en met meer resultaten? Het antwoord ligt in leiderschap dat een onderscheidend criterium is voor succesvol transformeren. Leiderschap in de verbinding tussen de interne organisatie en de externe politiek en ketenspelers.

Trends in Mobiliteit 2009

Trends in Mobiliteit 2009 'In de ban van het overleven: een visie vanuit het oog van de orkaan' is het derde rapport over ontwikkelingen in het mobiliteitsdomein dat Capgemini dit jaar in samenwerking met Transumo heeft gepubliceerd. Daar waar in eerdere rapporten specifiek werd ingegaan op de Nederlandse vervoerscapaciteit en de groeiende congestie buiten de Randstad, wordt dit jaar de samenhang tussen de fysieke en niet fysieke (lees: digitale) infrastructuur belicht. Daarnaast wordt gezocht naar redenen waarom infrastructurele projecten al dan niet succesvol zijn. Deze bevindingen kunt u vanzelfsprekend gebruiken voor het nemen van toekomstige besluiten.

Over Capgemini

Capgemini, wereldwijd een toonaangevende aanbieder van consulting-, technology- en outsourcingdiensten, stelt zijn klanten in staat te transformeren en betere prestaties te realiseren door middel van technologie. Capgemini verschaft nieuwe inzichten en mogelijkheden, waardoor klanten meer vrijheid krijgen om optimale resultaten te realiseren. Hierbij werkt Capgemini op een onderscheidende manier samen met zijn klanten: the Collaborative Business Experience™. Bovendien wordt gebruikgemaakt van het eigen wereldwijde leveringsmodel Rightshore®, dat op een evenwichtige manier getalenteerde professionals uit verschillende locaties samenbrengt in één team dat de best mogelijke oplossingen voor klanten creëert en levert.
Capgemini heeft vestigingen in meer dan 30 landen en heeft wereldwijd 95.000 medewerkers in dienst.
De organisatie realiseerde in 2009 een omzet van 8,4 miljard euro.
Meer informatie:
www.nl.capgemini.com

Rightshore® is een handelsmerk van Capgemini

Colofon

Trends in Veiligheid is mede tot stand gekomen met medewerking van:
Mr. Patrick de Graaf
Dietmar Griep
Petra Halenbeek
Drs. Erik Hoorweg MCM
Drs. Abderrahman Kaouass
Drs. Nico Kaptein
Mike Tettero
Drs. Geert de Vet
Drs. Saskia Wechseler

Capgemini Nederland B.V.
Papendorpseweg 100
Postbus 2575 - 3500 GN Utrecht
Tel.: 030 689 74 21
E-mail: trendsinveiligheid.nl@capgemini.com
www.capgemini.nl/veiligheid

IN/01-015.10/1000 © Hollandse Hoogte.nl

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.nl.capgemini.com

Capgemini Nederland B.V.
Papendorpseweg 100
Postbus 2575 - 3500 GN Utrecht
Tel. 030 689 00 00
Fax 030 689 99 99