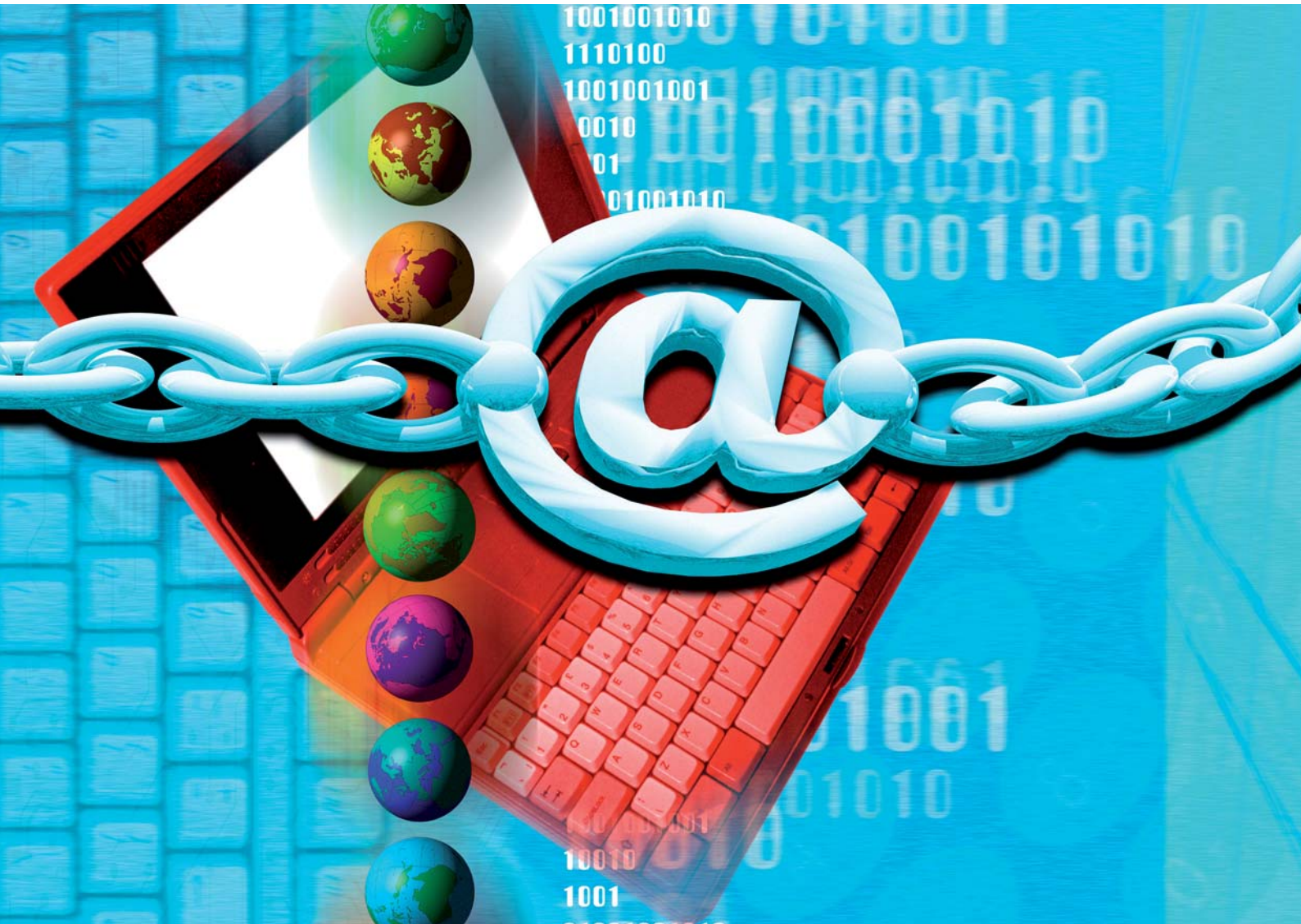
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

jaargang 7 | nummer 8 | **november/december 2009**

Magazine

nationale veiligheid en crisisbeheersing

Thema: Cybersecurity
Kritiek op griepcommunicatie: terecht of onterecht?
(Zelf)redzaamheid bij crises
Impressie EU Floodex 2009



Inhoud

THEMA: CYBERSECURITY

THEMA: (ZELF)REDZAAMHEID BIJ CRISES

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

Verder in dit nummer:

prof. dr. Peter Werkhoven,
directeur Kennis, TNO Defensie en Veiligheid

Cybersecurity – introductie

Het thema van deze special is Cybersecurity, een thema dat steeds belangrijker wordt in onze samenleving. Als de informatie- en communicatietechnologie (ICT) uitvalt, trekken bij veel bedrijven en overheden de medewerkers al binnen een uur gefrustreerd hun jas aan. Langdurige e-mailuitval lijkt voor enkelen zelfs traumatischer te zijn dan een echtscheiding. Ook de vitale infrastructuur is grotendeels afhankelijk van het goed functioneren van ICT. Bij grootschalige ICT-uitval vallen vitale functies weg, kunnen domino-effecten ontstaan en bestaat een substantieel risico op systeemfalen. Bij veel burgers komt dan de vraag op of Nederland voorbereid is op een grootschalige ICT-uitval of -verstoring. Hebben de private partijen en de overheid daar een crisisplan voor?

Reeds bij de vroegere voorlopers van het internet, het Arpanet van Defensie, was men zich bewust van veiligheidsproblemen. Begin jaren tachtig vond er drie keer maal per jaar overleg plaats tussen zes NAVO-landen (waaronder Nederland) over het internationaal synchroon upgraden van de Arpanet-routers. Recent werkten honderden Internet Service Providers in de hele wereld in onderling vertrouwen samen om een ernstige fout in de kern van het internet weg te nemen en zo misbruik te voorkomen. Toch kan een volgende keer niet worden uitgesloten dat een medewerker vroegtijdig kritische informatie lekt en de weg vrij maakt voor criminelen. Naast technologische beveiliging zijn ook gedrag en organisatie essentieel.

Cybersecurity strekt zich echter verder uit dan alleen het internet. Ook andere vormen van telecommunicatie zijn vitaal voor de samenleving. Zij kunnen, mede door de toenemende convergentie van tele-communicatiediensten, net zo goed getroffen worden door uitval en (on) opzettelijke verstoring. Cybersecurity nu vergt meer dan het oude achterkamertjes-overleg van enkele mensen die elkaar vertrouwen. Aanpak van cyber-onheil vereist nu internationaal samenwerken op grote schaal, overigens wel op basis van vertrouwen. Een sterke positie daarin als land, als private ICT-partijen, en als overheid is gewenst. Onze samenleving verwacht namelijk dat Nederland als innovatieve ICT-trendsetter voorbereid is om iedere vorm van onopzettelijke en opzettelijke ICT-verstoring het hoofd te kunnen bieden, ongeacht of deze nu veroorzaakt wordt door technisch falen, een menselijke fout, activisten (denk aan de aanvallen op Estland en aan Fitna) of door kwaadwillige staten (*cyberwar*). Nederland moet op ICT-gebied de continuïteit van haar samenleving en economie nu en in de toekomst kunnen waarborgen zonder voor die kennis afhankelijk te zijn van andere landen.

Daarnaast zal de ICT-veiligheidsbeleving van de burger en bedrijven hersteld moeten worden.

Dit themanummer gaat in op de vele proactie-, preventie-, preparatie-, incidentrespons- en incidentopvolgings-activiteiten op cybersecuritygebied die Nederland nationaal en in internationale dialoog uitvoert. Uit de bijdragen komt desondanks naar voren dat er nog zeer grote uitdagingen zijn op technisch vlak, op organisatorisch vlak, en op het vlak van bewustwording en ICT-veilig gedrag. Het Verenigd Koninkrijk heeft uit oogpunt van de bescherming van hun nationale veiligheid deze uitdagingen opgepakt met hun 'Cyber Security Strategy'. Voorbeeld doet volgen. Een soortgelijke krachtige Nederlandse kabinetsvisie op de aanpak van het gehele cybersecurity spectrum van spam en virussen tot en met cyberwar is nodig om onze cybersecurity ook in de toekomst te waarborgen. Hierbij moet al onze publieke en private kennis en kunde samengebracht en in stelling gebracht worden.

Mark Frequin, *DG Energie en Telecom, ministerie van EZ*
Dick Schoof, *DG Veiligheid, ministerie van BZK*
Hans van der Vlist, *DG Rechtspleging en Rechtshandhaving, ministerie van Justitie*

Samenwerking en **samenhang** maken het **verschil**

ICT en veiligheid

De ontwikkelingen op ICT-gebied gaan snel. Nederland loopt voorop als het gaat om gebruik van ICT. ICT is de digitale smeerolie in onze economie en is door gedrongen tot in de haarvaten van onze samenleving. We communiceren niet alleen via ICT maar duizenden processen als betalingsverkeer, vliegverkeer, industriële processen worden ook door ICT mogelijk gemaakt c.q. aangestuurd. ICT levert doorgaans gemak en verhoging van de productiviteit. Via de rijksbrede ICT-agenda willen we dit vasthouden en uitbouwen door in te zetten op o.a. innovatie, e-vaardigheden en toepassing van ICT in maatschappelijke domeinen.
Maar het succes van ICT heeft ook een keerzijde. We worden net als energie steeds afhankelijker en kwetsbaarder. ICT-uitval voelt als het wegvallen van een basisvoorziening. We kunnen haast niet meer zonder. Daarnaast wordt ICT helaas ook vaak misbruikt. Dagelijks worden we geconfronteerd met spam, malware en digitaal ongedierte als Trojaanse paarden, wormen etc. Niet alleen lastig maar ook schadelijk en soms zelfs ronduit gevaarlijk. De traditionele criminaliteit in een nieuw jasje: ICT wordt ingezet om bijvoorbeeld bankrekeningen te plunderen (phishing). Een ander voorbeeld is de inbreuk op integriteit van gegevensbeheer of beschadiging van netwerken.

Regie op ICT-veiligheid?

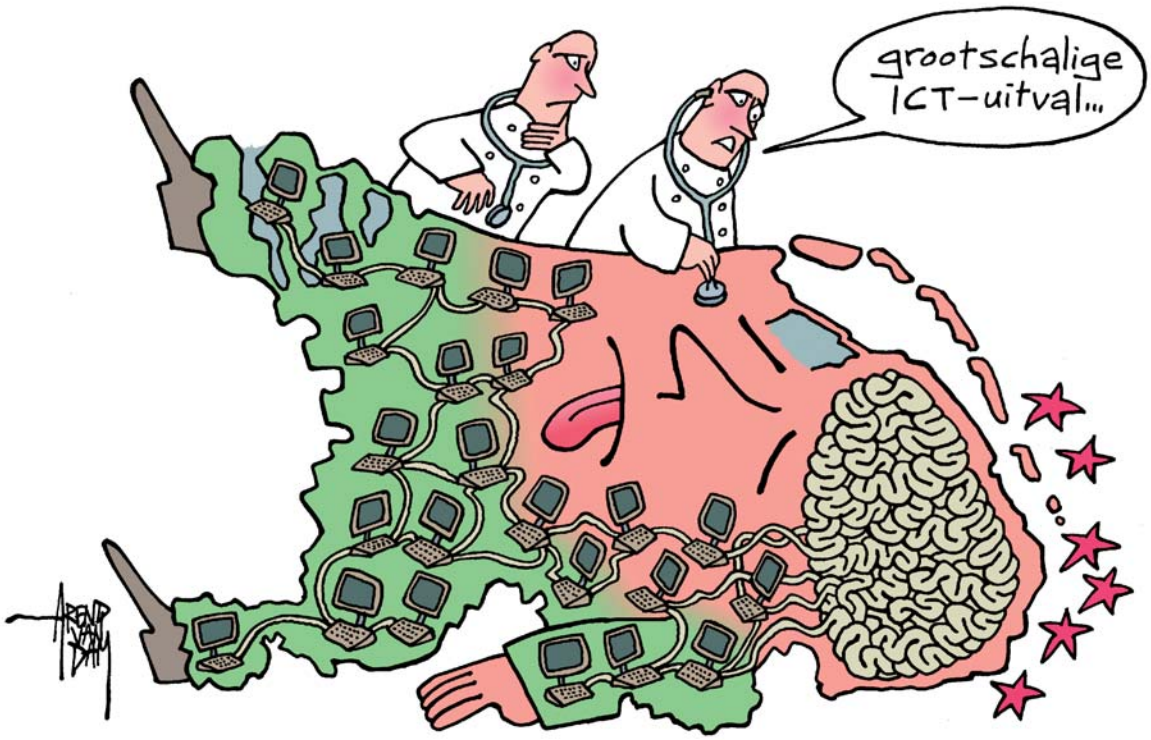
Digitale veiligheid is iets wat ons allemaal aangaat en dus moeten we er ook allemaal iets aan doen. Niet alleen overheid maar ook bedrijven en gebruikers. Daarin is het voor ons wel zoeken naar de juiste balans tussen publieke en private verantwoordelijkheid. De afgelopen jaren zijn verschillende programma's opgezet en projecten gestart met als doel de risico's, kwetsbaarheden en onderlinge intersectorale afhankelijkheden in kaart te brengen[1]. Verschillende organisaties zijn daarnaast al dan niet in PPS-verband actief in het voorkomen en bestrijden van cybercrime en het verhogen van de cybersecurity. Het speelveld en beleidsterrein is complex en voortdurend in beweging. Dit vraagt om goede afstemming binnen de overheid. BZK, EZ en Justitie vinden elkaar in het voorkomen van uitval en/of misbruik van ICT. Preventie is daarin een kernbegrip. Om hier structuur in aan te brengen is een preventie-aanpak gelanceerd.

Preventie

In onze preventie-agenda ICT en Veiligheid (2008-2010) draait het om bewustwording, bevorderen van de publiekprivate samenwerking, informatie- en kennis-deling en (zelf-)regulering. De belangrijkste pijlers zijn:

1 het vergroten van bewustzijn en kennis van consumenten, gebruikers, bedrijven, organisaties en overheid over veiligheidsrisico's bij het gebruik van ICT en mogelijkheden zich daartegen te beschermen. Dit doen we bijvoorbeeld via het programma Digibewust en Digivaardig (www.mijndigitalewereld.nl) en de PB51-campagne "Veilig internetten " van afgelopen zomer.
2 het invullen van de eigen verantwoordelijkheid door organisaties en bedrijven door maatregelen om schade en overlast te beperken en waar mogelijk te voorkomen. Mooi voorbeeld hiervan is proces control security: de veiligheid van besturingssystemen die dwars door onze samenleving lopen en waar we dagelijks mee te maken hebben (elektronisch betalingsverkeer, verkeersgeleidingsystemen etc.). Vrijwel alle (al dan niet vitale) sectoren zijn in belangrijke mate van eigen ICT én openbare netwerken afhankelijk. Hier is de sleutel samenwerking met het bedrijfsleven (PPS). Geheel ander voorbeeld: de gedragscode Notice-and-Take-Down op basis waarvan aangesloten organisaties actief illegale sites uit de lucht halen.
3 het waarborgen en continueren van PPS door inrichting van gestructureerd overleg en een gezamenlijke gedragen aanpak. Voorbeeld: het Strategisch Overleg Vitale Infrastructuren, het NICC-programma en het binnenkort te starten platform Internetveiligheid.
4 ontsluiting en gebruik van kennis, zowel internationaal als nationaal van o.a. trends en ontwikkelingen van de technologie, de markt en het ICT gebruik, de risico's en mogelijke strategieën. Voorbeeld: het ontwikkelen van ICT scenario's in het kader van de Nationale Risicobeoordeling (NRB) en een haalbaar-heidsonderzoek naar een nationale trendrapportage cybercrime.

[1] Nationale Veiligheid, Bescherming Vitale Infrastructuur, Veiligheid begint bij Voorkomen.



Sturing ICT en veiligheid binnen het rijk

De uitvoering van al deze acties en plannen zijn onderdeel van ons gezamenlijk overleg, het zogeheten 3DG-overleg. Onze inzet is het gemeenschappelijke belang dat meer is dan de optelsom van de deelbelangen. Drie voorbeelden.

1 De afgelopen jaren hebben Govcert, NAVI en het programma NICC zich ingezet voor betere bescherming van vitale infrastructuren en het voorkomen van bijvoorbeeld cybercrime. Er is veel goed werk geleverd: er is beter inzicht in de intersectorale afhankelijkheden en kwetsbaarheden, er is een goed lopend Informatie-knooppunt Cybercrime en met Govcert hebben we een professionele en internationaal goed aangeschreven CERT in huis. Maar, er zit meer in en er is nog meer nodig gelet op sommige dreigingen. Zoals bij voorbeeld meer synergie tussen de operationele CERT-functie en de kennis- en informatiedelingsfunctie. Functies die elkaar voeden en kunnen versterken. Hier zien wij een mooie kans om deze krachten te bundelen in een nieuwe organisatie die werkt volgens de principes van PPS. Wij zijn overtuigd van de meerwaarde ervan en willen de vorming van een nieuwe organisatie een kans geven. Een organisatie die vooral aan de voorkant werkt. Daar vinden wij elkaar. Werken aan de voorkant levert hopelijk minder werk aan de achterkant op: opsporing en vervolging. De komende maanden wordt aan het ontwerp en de inrichting ervan gewerkt. Tijdens de verbouwing moet uiteraard de winkel blijven draaien. Dat betekent vooral dat het goede werk vanuit het programma NICC en het NAVI wordt voortgezet. Medio 2010 zou de nieuwe organisatie moeten draaien.
2 De brede wens om te komen tot een nationale trendrapportage cybercrime. Veiligheid is lastig te kwantificeren, zeker als het gaat om digitale veiligheid. De indruk bestaat dat vaak vanuit een 'onderbuik-gevoel' wordt gehandeld. Effectieve sturing vraagt om cijfers en trends. Waar gaat het naar toe? Wat zijn hypes en wat zijn onderliggende structurele ontwikkelingen? Afgezien van vele rapporten en studies binnen overheid en bedrijfsleven over virussen, malware etc., ontbreekt het aan een separaat trendrapport op strategisch niveau. Een rapport dat 1 á 2 jaar vooruit kijkt en de basis vormt voor beleidskeuzes. Een rapport dat ons ook kan helpen in de beleidscommunicatie over de samenhang tussen veiligheid en ICT. Veel initiatieven kennen namelijk een zelfde aanpak – zoals het uitwisselen van informatie via platforms – waarmee de output wel bekend is maar de outcome eigenlijk niet. We mikken op een eerste trendrapport medio 2010.
3 Derde voorbeeld is de afspraak om meer gezamenlijk te oefenen rond het thema ICT-uitval. Nederland zal participeren in de Amerikaanse oefening Cyberstorm III, waarbij ook onze bewindspersonen betrokken zullen worden. Op die manier blijft het onderwerp tot op het hoogste niveau op de agenda.

Tot slot

Veiligheid van onze ICT is een complex vraagstuk en is een zaak van ons allen. Gelet op de dynamiek van de sector (nieuwe spelers), de verwevenheid van ICT in onze samenleving en de snelheid van technologische ontwikkelingen, is een continue dialoog met het veld van belang. Rode draad in onze benadering is dus vooral het creëren van bewustwording, faciliteren van netwerken en samenwerkingsverbanden (PPS-constructies) en promoten van zelfregulering. In de sturing hierop kunnen rapportages, monitoring en op termijn effectmeting helpen om de houdbaarheid van de interventies te bepalen. We moeten voorkomen dat beleids-instrumenten ingesleten raken en als vanzelfsprekend worden ervaren. De wereld om ons heen draait namelijk door. Die omgevingsdynamiek en het maatschappelijk belang van digitale veiligheid, houdt ons scherp en maakt het werk spannend!

Wereldwijde ervaringen met **ICT-uitval en -verstoringen**

ir. Eric Luiijf,
principal consultant Information Assurance en Bescherming vitale infrastructuur, TNO Defensie en Veiligheid (eric.luiijf@tno.nl)

Grootschalige ICT-uitval of -verstoring met effecten op een regio, Nederland of wereldwijd, kan ernstige gevolgen hebben voor de veiligheid en het welbevinden van burgers en kan leiden grote economische schade. Op basis van de TNO database waarin vitale infrastructuurverstoringen en de domino-effecten daarvan worden geregistreerd gaat dit artikel nader in op dergelijke uitval en -verstoringen en de (inter)nationale voorbereidingen op ICT-rampen.

Informatiesystemen

Grootschalige uitval van informatiesystemen komt vaak voort uit de afhankelijkheid van elektriciteit. Een paradox daarbij is dat in gebieden waar de elektriciteitsvoorziening met enige regelmaat faalt minder vaak domino-effecten optreden in de telecommunicatiesector dan in gebieden waar de energieleveringszekerheid hoog is zoals in Nederland.[1] Internationaal vormt het Strategisch Overleg Vitale Infrastructuur (SOVI) een uitzondering waar de domino-effecten van elektriciteitsuitval op ICT en de mogelijke maatregelen daartegen besproken intersectoraal worden besproken.

Een andere oorzaak van grootschalige uitval van informatiesystemen vormt de razendsnelle internationale verspreiding van virussen en andere 'malware'. De laatste jaren zorgen geavanceerde detectie- en quarantaine-mechanismen in bijvoorbeeld e-mailstromen voor vroegtijdig ingrijpen. Wereldwijde besmettingen met grote verstoring van IT-systemen treden desondanks op. In het buitenland zijn al (petro)chemische fabrieken en kerncentrales uitgevallen. Ook is de controle over elektriciteitstransportinfrastructuren verloren doordat de procescontrolesystemen en -netwerken met malware besmet raakten. Dergelijke incidenten komen soms voort uit onverstandige verbindingen met het internet, Vaker komt de besmetting door besmette laptops van derden die 'onveilige gemeenschap' hebben met vitale productienetwerken. De mogelijk gevolgen kunnen, mede door domino-effecten, heel ernstig zijn. In het Informatieknooppunt Cybercrime (IKC) en internationale samenwerkingsverbanden (EuroSCSIE en MPSCSIE) werken de Nederlandse vitale sectoren samen om dit risico in te dammen.

Daarnaast zijn er de IT-kwetsbaarheden die grootschalig uitgebuit worden door criminelen, bijvoorbeeld voor het opzetten van botnets of het verzamelen van persoonlijke gegevens. De betrouwbaarheid van en vertrouwen in IT-diensten komt daarbij in het geding. Internationaal werken Computer Emergency Response Teams (CERTs) en opsporingsdiensten samen om

[1] A.H. Nieuwenhuijs, H.A.M. Luiijf, M.H.A. Klaver, 'Modeling Critical Infrastructure Dependencies', in: P. Mauricio and S. Shenoi (eds.), IFIP Volume 290, Critical Infrastructure Protection II, October 2008, 205-214.

dergelijke cybercriminaliteit enigszins in te dammen en bij ernstige verstoring samen op te trekken en kennis te delen.

Internettoegang en -diensten

Internet is door zijn opzet robuust en kan als totaal systeem niet uitvallen. Wel kunnen delen uitvallen. Dat komt door single-point-of-failures (SPoFs) of door overbelaste circuits waar geen redundante capaciteit elders in het netwerk voor bestaat. Wordt dan de zeekabel (bijv. de SEA-ME-WE) doorsneden door een aardbeving of een anker, of zijn er grote (distributed) denial-of-service aanvallen, dan zijn zelfs landen elektronisch gezien niet of nauwelijks te bereiken. Ook ISP, telecom-, en CATV-operators zien SPoFs over het hoofd, wilden niet investeren in redundantie, of moesten van de gemeente alle glaskabels in één tracé neerleggen. Uitval van honderdduizenden tot enkele miljoenen klanten voor langere tijd komt voor. De kwetsbaarheid van dergelijke SPoFs kan ook uitgebuit worden voor activistische of criminele doeleinden. Voor de lokale Internettoegang geldt hetzelfde. Als men geen tweede toegang via een bewijsbaar andere route heeft geregeld, kan het internet uitvallen inclusief alle diensten als e-mail, web en internettelefonie. Ook de crisisrespons-organisaties zijn vaak optimistisch en zien SPoFs over het hoofd.[2]

Vaste en mobiele telefonie- en datadiensten

De nieuwe cultuur van 'always anywhere on-line' brengt het risico van een lage tolerantie voor verstoringen. Bedrijven en burgers zijn geheel van slag als hun Blackberry niet minstens drie e-mailberichten per uur toont. Laat staan dat die dienst zo'n 12 uur uitvalt zoals in 2007 gebeurde. Men kan niet e-mailen en e-mail ontvangen: men bestaat niet meer!
Uitval van vaste en mobiele communicatie wordt vaak veroorzaakt door noodweer en rampen als aardbevingen of overstromingen. Naast de technische uitval van componenten ontstaat daarbij overbelasting doordat velen tegelijk willen communiceren. Als netwerken meer diensten leveren, zal een overbelasting in één dienst al gauw congestie van een andere telecommunicatiedienst veroorzaken. Als de normale beschikbaarheid 99.99% is, maakt een communicatie-inspanning over mogelijke ICT-uitval tijdens bijzondere omstandigheden geen indruk, noch in het buitenland, noch in Nederland: het zal zo'n vaart niet lopen.
Analyses van rampen laten zien dat na herstel van de infrastructuur een 30% hogere netwerkbelasting gemeten wordt dan voor de ramp. Omdat men zich ongerust maakte over familie en kennissen wordt er vaker gecommuniceerd, een effect dat zich gedurende meer dan een jaar voortzet. Een aantal landen heeft zijn ontwerpcriteria hierop aangepast.

Technische storingen en menselijke fouten brengen SPoFs in de infrastructuur aan het licht zoals kwetsbare locaties en gateways met andere operators. Systeemupgrades en onvoorziene extra netwerkbelasting omdat men de abonnees ineens hogere snelheid biedt, hebben in de afgelopen jaren geleid tot onvoorziene neveneffecten en langdurige, grootschalige ICT-uitval. Een beperkt aantal landen heeft een publiek-privaat crisisplan en -organisatie voor de hele ICT-sector, bijvoorbeeld de Special Task Force on Information Assurance (SONIA) in Zwitserland en het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T) in Nederland.
De perceptie van een hoge betrouwbaarheid van veel nieuwe communicatie- en datadiensten maakt dat wij onszelf afhankelijk van die diensten maken. We vergeten daarbij dat de dienstverlening niet betrouwbaarder kan zijn dan die van de onderliggende infrastructuur en techniek. Rampbestrijdingsorganisaties in Nederland en daarbuiten trappen wel eens in deze val en zijn afhankelijk van overbelastinggevoelige netwerken met SPoFs.

ICT-rampbestrijding

Qua preventie en preparatie analyseert het VS National Infrastructure Simulation and Analysis Center (NISAC) met simulatiemodellen onder andere de kans op ICT-uitval per regio en de mogelijke gevolgen van een volgende wervelstorm. In Europa en Nederland zijn we nog niet zover, ook al werkt TNO in het EU project DIESIS aan de contouren van een dergelijke Europese en Nederlandse faciliteit.
Qua preparatie en respons hebben veel landen CERT-organisaties die hun overheid en/of vitale sectoren helpen bij het wegnemen van ICT-kwetsbaarheden en bij de aanpak van incidenten. Een aantal landen, waaronder de VS, het VK, Estland en Zuid-Korea, ontwikkelt daarnaast beleid en een responsorganisatie voor de nationale bescherming tegen Cyberwar. Dit mede naar aanleiding van de recente Cyberaanvallen op Estland, Georgië, Kirgizië en Zuid-Korea. Ze oefenen grootschalig op oefeningen om cyberaanvallen te weerstaan (bijv. Cyberstorm in de VS). Ook Nederlandse ICT-systemen en -netwerken worden aangevallen vanuit het buitenland. Over de vele partijen die zich in meer of mindere mate samen bezig houden met de ICT-rampbestrijding in Nederland kunt u elders in dit magazine meer lezen.

[2] E. Luiijf and M. Klaver, 'Insufficient Situational Awareness about Critical Infrastructures by Emergency Management', in: *Proceedings Symposium on "C3I for crisis, emergency and consequence management, Bucharest*, May 2009, NATO RTA, Paris. RTO-MP-IST-086.

Bart Jacobs,
hoogleraar computerbeveiliging Radboud Universiteit Nijmegen (www.cs.ru.nl/~bart)

Pas op: **in je blootje vat je kou!**

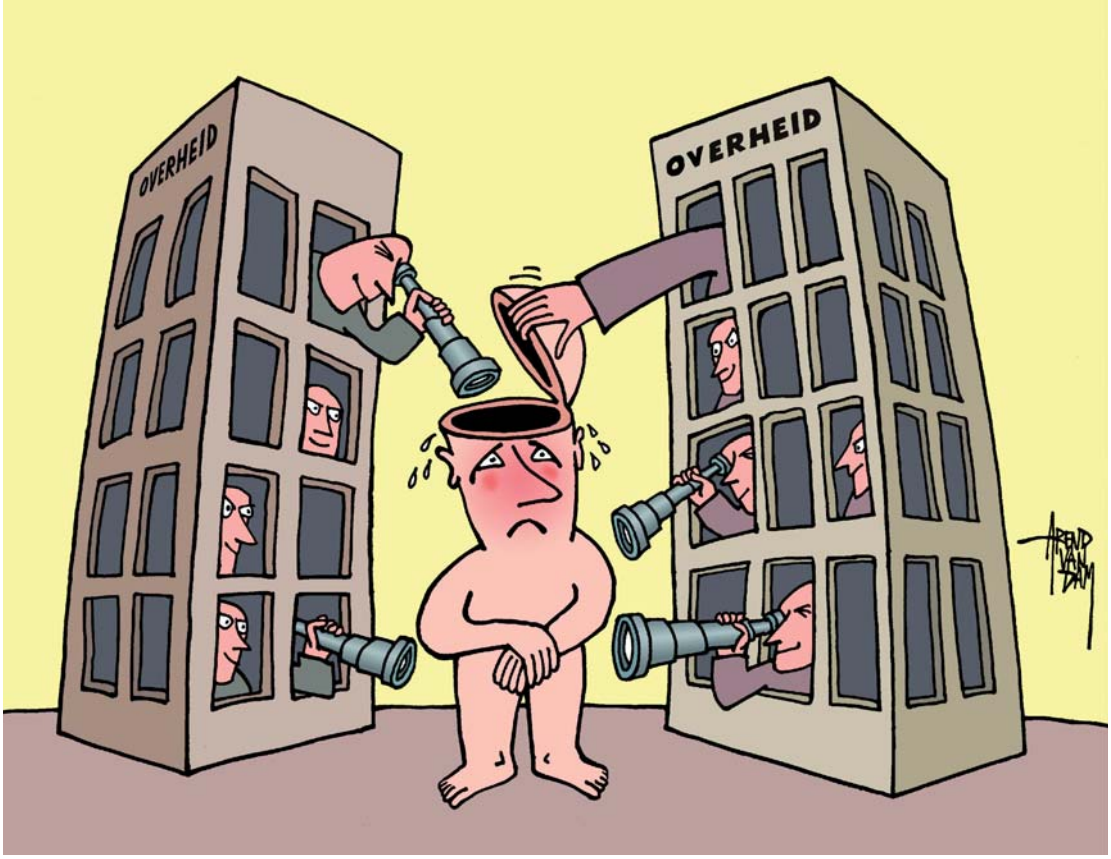
Begin september 2009 waarschuwde de Amerikaanse president Obama jongeren om vooral geen gekkigheden over zichzelf op sociale netwerken te plaatsen, zeker als ze de ambitie hebben om ooit president van de Verenigde Staten te worden. Als jongere doe je soms domme dingen, zei Obama, die je online kunnen blijven achtervolgen, zoals bij sollicitaties. Dit geldt voor veel ambten, en niet alleen voor het hoogste.
De Nederlandse overheid was er in de zomer van 2009 eerder bij. Toen werd de campagne "Veilig Internetten" in gang gezet om de eigen burgers voor soortgelijke risico's te waarschuwen (zie website www.veiliginternetten.nl). Vanaf een camping gaf minister van Justitie Hirsch Ballin het startschot voor een serie van TV-spotjes om mensen beter bewust te maken van de persoonlijke gegevens die ze op internet zetten en van de kwetsbaarheden die ze daarmee mogelijk creëren. Een voor de hand liggend voorbeeld is het openlijk vermelden van niet alleen het eigen huisadres maar ook de vakantiedata op sociale netwerksites zodat inbrekers daar hun voordeel mee kunnen doen. Dit is een zinvolle en hoognodige campagne.
Toch schuurt en jeukt er iets.
Diezelfde overheid heeft de afgelopen jaren wetgeving en maatregelen ingevoerd waardoor velerlei gevoelige persoonlijke informatie van ons burgers vastgelegd en ingeleverd moet worden, via bijvoorbeeld dataretentie (van email en telefoonverkeer), elektronische slotgrachten (waarmee autokentekens automatisch geregistreerd worden), centrale opslag vingerafdrukken (uit paspoorten), opslag van openbaar vervoersbewegingen (voor 7 jaar, via OV-chipkaart), elektronische `smart' meters (die iedere 15 minuten het elektriciteitsgebruik automatisch doorgeven), etcetera. Eerst worden ons door de overheid de kleren van het lijf getrokken, en vervolgens krijgen we te horen: "pas op, in blootje vat je kou!".
Is hier sprake van hypocrisie?

Good guys en bad guys

Impliciet bij deze ontwikkelingen is een aantal vooronderstellingen, met name over wie *good guys* en *bad guys* zijn. De overheid waarschuwt ons tegen *bad guys* die mogelijk misbruik maken van onze persoonsgegevens, maar beschouwt zichzelf nadrukkelijk onderdeel van de *good guys*. De situatie zou als volgt explicieter gemaakt kunnen worden. De overheid zegt: "Brave burger, verspreiding van persoonsgegevens maakt u kwetsbaar; daar kan op allerlei manieren door kwaadwillenden misbruik van gemaakt worden. Maar die persoonsgegevens moet u wel bij ons in leveren zodat we u beter kunnen helpen en beschermen; overheden zijn goedwillend en maken nooit misbruik van zulke gegevens." Deze formulering schuurt en jeukt al veel harder.
Om te beginnen is het een positieve ontwikkeling dat de overheid burgers waarschuwt voor de risico's van slordige omgang met persoonsgegevens. Vroeger was het zo dat je vooral zelf een sukkel was in geval van slordigheid. Identiteitsfraude kan echter zodanige vormen aannemen dat het maatschappelijk ontwrichtend kan werken, bijvoorbeeld wanneer grootschalige administraties en bestanden vervuild raken door propagatie van fouten. Dit zou mogelijk kunnen optreden bij identiteitsfraude in de zorg (door onverzekerden) waardoor foutieve medische gegevens zich via landelijke koppelingen voortplanten. Ook is de huidige infrastructuur voor financiële dienstverlening in hoge mate afhankelijk van adequate authenticatie van personen, bijvoorbeeld bij internetbankieren. Indien deze authenticatie in een significant aantal gevallen faalt, hebben we nauwelijks meer een alternatieve infrastructuur om op terug te vallen. Daarnaast kunnen zaken die geheim zouden moeten blijven, mogelijk uitlekken door ondoordachte verspreiding, zoals bij voorbeeld de identititeit van de chef van de Britse geheime dienst MI6, die normaal alleen als "C" bekend is, maar deze zomer door toedoen van zijn echtgenote slechts in zwembroek te zien was op Facebook.
Er is dus alle reden voor terughoudendheid met persoonsgegevens. In feite behoort het aanleren van dergelijke terughoudendheid tot de basisvaardigheden die (jonge) mensen zich eigen moeten maken in het digitale tijdperk.

Burgers leveren in

Des te wranger is het dat de overheid in steeds sterkere mate aanstuurt op transparantie van burgers – en veel minder andersom, overigens. Om vage redenen worden zware inleververplichtingen opgelegd, zonder dat daar duidelijk meetbare doelstellingen, evaluaties, of inschattingen met betrekking tot risico's of misbruik tegenover staan. Heeft de politie bijvoorbeeld een meetbare doelstelling om aantoonbaar X procent meer zaken op te lossen door de digitale slotgrachten, en is ze bereid om in geval dat percentage niet gehaald wordt de kenteken-camera's weer te verwijderen? Natuurlijk niet. Het gebrek aan een dergelijke kritische context versterkt het wantrouwen en het risico op steeds uitgebreider gebruik, veel verder dan de oorspronkelijke doelstellingen – *if any*.
Een goede illustratie van dergelijke *function creep* vormen de vingerafdrukken in paspoortchips. De oorspronkelijke



Overheid: "good guys" of "bad guys"...?

doelstelling om daarmee de band tussen een paspoort en de drager ervan beter te kunnen controleren is goed te verdedigen. Gaandeweg zag de overheid echter nieuwe "kansen" en besloot de vingerafdrukken zelf op te slaan in een centrale database. Daarvoor werden gekunstelde redenen bedacht, zoals het voorkomen van het aanvragen van twee paspoorten onder verschillende naam – zonder te onderzoeken hoe groot dat probleem eigenlijk is – of identificatie van slachtoffers bij grote rampen – waarvoor gebitten natuurlijk veel geschikter zijn dan vingerafdrukken. Na enige tijd kwam de aap uit de mouw: inlichtingendiensten en justitie willen ook in de database kunnen zoeken! In de wet zoals die er nu uitziet staan nog allerlei procedurele beperkingen voor toegang door justitie. Maar je hoeft geen helderziende te zijn om te weten dat die beperkingen er snel van af gaan. Het scenario is voorspelbaar: eerst komt er een hoofdcommissaris van politie op TV vertellen dat zware-jopie-de-serie-baby-verkrachter op tijd gepakt had kunnen worden als men zonder beperkingen toegang tot de database had gehad en vervolgens gaat de politiek door de knieën. Binnen een paar jaar fungeert deze centrale database met vingerafdrukken als een kenteken-register voor alle burgers – en niet alleen de criminele. Onduidelijke doelstellingen en vormen van *function creep* bij informatieverzameling dragen niet bij aan vertrouwen en maken het minder vanzelfsprekend dat de overheid tot het kamp van de *good guys* behoort.

Bescherming van burgers

Natuurlijk worden wij burgers geacht de overheid tot de *good guys* te blijven rekenen, bij wie wij dus zonder aarzeling en zorgen onze persoonsgegevens wel kunnen inleveren. Het lijkt het voorstellingsvermogen van veel Haagse politici te boven te gaan dat burgers misschien ook tegen de eigen overheid beschermd zouden moeten worden. Het is zorgelijk wanneer de overheid zonder duidelijke motivatie zo sterk inzet op het in de gaten houden van de eigen burgers met middelen die niet anders gekwalificeerd kunnen worden dan als instrumenten van een politiestaat. Een eventuele minder welwillende overheid komt hierna in een gespreid bedje. Maar, zult u misschien tegenwerpen, al deze maatregelen zijn toch niet tegen burgers gericht maar worden juist ingevoerd om de veiligheid te vergroten en de burger te beschermen. Dit pad van steeds ingrijpender surveillance en controle, via instrumenten van een politiestaat, heeft echter een eigen logica en dynamiek, waarbij we aan het eindpunt mogelijk tevreden kunnen constateren dat een politiestaat voor veel mensen veiliger is dan een democratie. Onze tijd vraagt om een heldere visie met bijbehorend toetsingskader, om grenzen te kunnen en durven stellen en om een balans te vinden tussen enerzijds door angst en effectiviteitseisen gedreven surveillance en controle en anderzijds bescherming van individuele autonomie. Misschien is het voor de overheid een zinvolle aanvulling op de campagne om de technologische voortgang ook (en vooral) in te zetten om die autonomie te beschermen en te versterken.
Het is een belangrijke stap dat de huidige overheid de risico's van onzorgvuldige verspreiding en gebruik van persoonsgegevens inziet en burgers daar nadrukkelijk tegen waarschuwt. Geloofwaardigheid van deze waarschuwing legt de overheid zelf ook de nodige verplichtingen op, niet alleen in handelen maar ook in verantwoording. Om de impliciete vooronderstelling bij deze waarschuwing dat de overheid zelf tot de *good guys* behoort en blijft behoren waar te maken is een andere houding en werkwijze nodig dan de afgelopen jaren ten toon gespreid is.
Anders wordt het tijd voor een nieuw type waarschuwingsspotje.

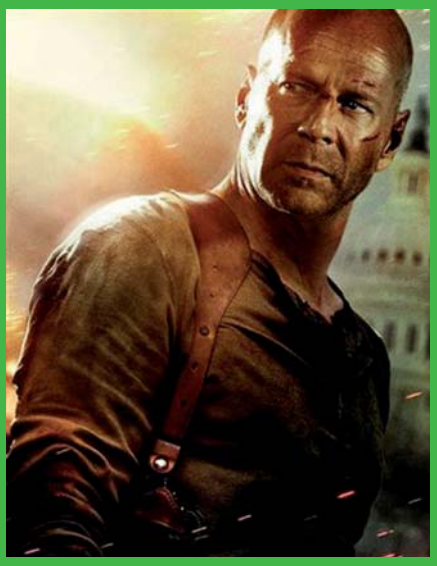
Bruce Willis in de polder

Of:

Hoe weerbaar

zijn vitale sectoren tegen uitval van ICT en electriciteit?

Hans Oude Alink
(namens het projectteam van NAVI, NICC, EZ en BZK)



Wel eens de film Die Hard IV met Bruce Willis in de hoofdrol gezien? Je zal met enig ongeloof hebben gekeken naar de omvang van de schade die een groep terroristen aan de samenleving kan toebrengen door ICT-systemen te manipuleren of uit te zetten. De stroom valt massaal uit. Verkeerssystemen worden in de war geschopt. De financiële wereld wordt onderuit gehaald. De telefoon werkt niet meer. En ga zo maar door. Gelukkig is Bruce praktisch in zijn eentje en met gebruikmaking van veel geweld in staat om de samenleving voor een totale ondergang te behoeden.

Natuurlijk maakt Hollywood een dergelijk scenario groot en spectaculair. Toch wordt met deze film een thema aangesneden waar sinds enige tijd ook de overheid en het bedrijfsleven zich steeds drukker om maken. De samenleving wordt, naast de al langer bestaande afhankelijkheid van elektriciteit, ook steeds afhankelijker van ICT en uitval zal een grotere impact krijgen. In het programma Nationale Veiligheid is dit uitgezocht en de conclusie van deze analyses is dat ICT-uitval naast grootschalige elektriciteitsuitval tot de grotere risico's voor de samenleving behoort. De economische schade kan in de vele miljarden lopen en

2010 – Jaar van de ICT

projectteam Digitale veiligheid, ministerie van BZK

2010 wordt voor DGV het Jaar van de ICT. Vanuit de directie Nationale Veiligheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt het komende jaar extra aandacht besteed aan het onderwerp digitale veiligheid. Met organisaties binnen en buiten BZK, waaronder het ministerie van EZ en publieke en private partijen, wordt onder de noemer "digitale veiligheid" een breed project opgezet met als doel het verbeteren van de weerbaarheid tegen uitval van ICT en elektriciteit. Binnen dit project worden bestaande trajecten voortgezet en nieuwe ontwikkeld. Zo wordt gewerkt aan de verbetering van de respons op uitval van ICT, uitmondend in een oefening in de tweede helft van 2010. Nederland doet mee aan de oefening Cyberstorm III die de VS organiseren om hun ICT-responsplan te oefenen. Ook is ICT opnieuw een thema in de cyclus van scenario-ontwikkeling, risicobeoordeling en capaciteiten-analyse van het programma Nationale Veiligheid.

De laatste jaren wordt vaker aandacht besteed aan specifieke thema's. Zo is dit jaar, evenals vorig jaar, onder andere met het ministerie van VWS, ingezet op de verbetering van de continuïteit van bedrijven en organisaties in geval van een grieppandemie. Eerder is met onder andere het ministerie van VenW en decentrale overheden in de Taskforce Management Overstromingen geïnvesteerd in de verbetering van de respons op overstromingen.

het sociaal-maatschappelijke leven kan ontwricht raken omdat veel alledaagse voorzieningen niet meer zullen werken. Kortom: omstandigheden die we niet willen.

Drie vragen

De voortgangsbrief Nationale Veiligheid, die afgelopen juni door het kabinet naar de Tweede kamer is verzonden, gaat hierop in. Enerzijds wordt ingezet op het weerbaarder maken van alle vitale sectoren tegen uitval van Telecom/ICT en elektriciteit en anderzijds is vastgesteld dat de respons op een mogelijke uitval van een van beide voorzieningen moet worden versterkt. Elders in dit magazine zal op dat laatste meer in detail worden ingegaan. Het eerste voorstel wordt nu door het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en het programma Nationale Infrastructuur Cybercrime (NICC) gezamenlijk opgepakt. De volgende vragen liggen voor:

1. Wat zijn de *kritische kernprocessen* binnen een vitale sector/organisatie, waarvoor het gebruik van elektriciteit dan wel Telecom/ICT van wezenlijk belang is?
2. Zijn er voor deze processen maatregelen getroffen bij uitval van Telecom/ICT of elektriciteit of te wel hoe *zelfvoorzienend of zelfredzaam* is de vitale sector/organisatie? En zo ja, hoe lang kunnen deze maatregelen worden volgehouden?
3. Welke *aanvullende maatregelen* kunnen worden getroffen?

Dit jaar worden de sectoren Energie, Telecom/ICT en Financiën onder de loep genomen, volgend jaar volgen de andere sectoren.

Eerste bevindingen

Uit de eerste gesprekken met vertegenwoordigers uit die sectoren blijkt dat zij zich terdege bewust zijn van hun afhankelijkheid van Telecom/ICT en/of elektriciteit. Zonder elektriciteit kan de telecomsector maar gedurende een korte periode doordraaien. Andersom is de afhankelijkheid net zo groot. Bij grootschalige uitval van elektriciteit is telecommunicatie van cruciaal belang om het netwerk te herstellen. Deze wederzijdse afhankelijkheid zien de sectoren zelf ook. Zij steken dan ook extra inspanning in dit traject omdat ze hun eigen business continuïteit daarmee kunnen verbeteren. Zij willen wel zo concreet mogelijke resultaten boeken. Zo worden bijvoorbeeld nu al herstelplannen nader tegen het licht gehouden.
De financiële sector is sterk afhankelijk van zowel de elektriciteit als de telecom/ICT. Zo is bijvoorbeeld een ononderbroken gebruik van elektriciteit en ICT van vitaal belang voor de continuïteit van het betalingsverkeer. Consumenten vertrouwen op een soepel lopend betalingsverkeer in onder andere winkels, uitgaansgelegenheden en tankstations; maar denk ook aan salarisbetalingen. Er zijn natuurlijk al diverse maatregelen getroffen door de financiële sector, zoals bij voorbeeld rondom het gebruik van beveiligde toegang bij internetbankieren. Samen met deskundigen uit de telecom/ICT en elektriciteitsector worden binnen dit traject deze bestaande maatregelen getoetst en daar waar nodig aangevuld.

Extra maatregelen nodig?

De mensen uit de verschillende sectoren beginnen elkaar nu echt te vinden en aan te spreken op elkaars rol in het overeind houden van vitale functies in de samenleving. Dat is de winst die nu al merkbaar wordt. Volgens de planning zullen aan eind van het jaar de eerste resultaten bekend worden en zal blijken of er aanvullende maatregelen worden voorgesteld. In 2010 zullen andere vitale sectoren worden benaderd. Dan moet blijken of Bruce Willis alsnog in de polder moet optreden of dat we ons als samenleving voldoende weerbaar hebben gemaakt.

Optreden bij grootschalige ICT-verstoringen: meer succes met

ICT Response Board

Douwe Leguit, GOVCERT.NL

Het vraagt meer dan één man, zelfs al ben je Bruce Willis, om grootschalige ICT-verstoringen te tackelen. Sterker nog, het vereist samenwerking met vele partijen binnen de overheid en de private sector om te komen tot een effectieve bestrijding. Immers, ICT is zo verwoven in onze samenleving dat een ICT verstoring bij de ene partij impact kan hebben op de andere en vice versa. We zijn van elkaar afhankelijk geworden. Ook wanneer het gaat om een goede respons op ICT-verstoringen.

Op de vraag hoe de respons bij grootschalige ICT-verstoringen aan te pakken, is een nieuw concept naar voren gekomen: de ICT Response Board (IRB). De gedachte is dat verschillende partijen en expertisegroepen bij ICT-calamiteiten aan tafel schuiven, om gezamenlijk te komen tot goede analyse van de situatie en een voorstel voor de te ondernemen acties. Daarbij ligt de focus op ICT-verstoring en niet op de bestrijding van de gevolgen daarvan in de werkelijke wereld (bij voorbeeld ordeverstoring). Insteek is dat de crisisorganisaties binnen het Rijk bij ICT-calamiteiten met een maatschappelijke impact snel tot weloverwogen besluitvorming kunnen komen, opdat de schade beperkt blijft en verstoringen snel verholpen worden.

In de dagelijkse gang van zaken worden (potentieel) grootschalige incidenten aangeleverd aan de IRB, welke in een kleine groep (die ook als "waakvlam" optreedt) triage zal uitvoeren om te bepalen of en zo ja hoe een incident tot mogelijk een maatschappelijke ontwrichting kan leiden. Indien dat het geval is, zal de IRB opgeschaald worden. De relevante partijen vanuit de publieke en private sector zullen worden uitgenodigd om plaats te nemen in de IRB om een gedetailleerdere analyse van de situatie op te stellen, met bijbehorend voorstel hoe te reageren (respons). Ook voor de uitvoering en coördinatie, van de daadwerkelijke operationele ICT-respons bij zo'n calamiteit, zal PPS noodzakelijk zijn. Immers, de netwerken en vitale infrastructuren zijn grotendeels in private handen.

In de opzet van de IRB zijn dan ook verschillende belanghebbenden voorzien: ICT-dienstverleners en -leveranciers, uitvoeringsorganisaties van de overheid, vitale sectoren en de daaraan gekoppelde vakdepartementen. Het is de synergie van de reeds aanwezige kennis, expertise, ervaring en capaciteit die het mogelijk maakt om de situatie snel te analyseren en tot gerichte voorstellen voor acties te komen. De IRB biedt dus vooral een versterking van de huidige crisisorganisaties met deze ondersteunende functie op het vlak van ICT. Daarbij dient wel gezocht te worden naar een oplossing voor een aantal vraagstukken:

- Hoe wordt de "waakvlamfunctie" ingevuld in rustigere tijden?
- Wanneer en welke incidenten worden aangemeld?
- Hoe geschiedt de eerste triage en wie doet dat?
- Wanneer wordt er opgeschaald en met wie?
- Hoe deelnemers van de IRB vrij te maken ten tijde van crisis?
- Hoe kan er gecommuniceerd worden ten tijde van crisis?
- Op welk moment wordt de verbinding gezocht met de bestaande crisisstructuren?
- Welk mandaat heeft de respons board ten aanzien van coördinatie van IT-maatregelen?

GOVCERT.NL is door het ministerie van Economische Zaken en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gevraagd om begin 2010 een eerste uitwerking van dit concept te realiseren. Hiervoor zal contact gezocht worden met de diverse belanghebbenden. De aanpak van de IRB zal pragmatisch zijn met een flexibele opzet als streven, gebruikmakend van de resultaten en netwerken vanuit het project weerbaarheid tegen uitval van elektriciteit en ICT. Ook zullen de bestaande kanalen met vitale sectoren en ISP's en overige belanghebbenden meegenomen worden. De feitelijke inrichting van de IRB zou dan later in 2010 moeten geschieden. Een eerste stap is nu te komen tot een goed model voor de ICT Respons Board welke door alle partijen gedragen wordt. Want met alleen spierballen, veel explosieven en geluk komen we er niet...

Even je mail checken? Met een trage pc, stapels SPAM en popups dat je je software moet updaten is het verleidelijk om alles weg te klikken, want ach, wat maakt dat uit? Herkenbaar? Nu steeds meer mensen thuis en mobiel internetten en nu internet-criminelen zich steeds vaker en grootschaliger via mal- of spyware meester maken van pc's van anderen om SPAM te versturen, aanvallen uit te oefenen of systemen plat te leggen (*Govcert Trendrapport 2009*), leidt onveilig internetten echter snel tot een groei van het aantal slachtoffers van cybercrime en tot een digitaal onveiliger Nederland. De ministers van BZK en Justitie maken zich daar zorgen over en ze nemen diverse maatregelen. Ook private partijen dragen steeds meer hun steentje bij, maar hoe zit het met ons, burgers van Nederland?

Anja van Zantvoort,
beleidsadviseur preventie cybercrime, ministerie van Justitie

Veiligheid zoals burgers die ervaren

Postbus 51 campagne 2009 "Veilig Internetten"

Om het brede publiek te waarschuwen voor de risico's van onveilig internetten is in opdracht van de minister van Justitie in de zomer 2009 de postbus 51 campagne "Veilig Internetten" gestart om mensen te waarschuwen dat ze slachtoffer kunnen worden van cybercrime als ze onveilig internetten. Veel mensen hebben het tv-spotje gezien waarbij een vrouw op het dak van een winkelcentrum haar gegevens letterlijk van de daken schreeuwt en veel Hyves-gebruikers zijn geïnformeerd dat Stanislav en zijn cybermaffia ook hen in de gaten heeft. Niet alleen deze uitingen zelf, maar ook het effectonderzoek dat hiervoor is verricht is interessant.

Hoe wij burgers omgaan met onze persoonlijke digitale veiligheid blijkt namelijk uit metingen die de RVD voor deze campagne heeft verricht. Enkele highlights:

Volwassenen emailen, regelen bankzaken en doen online-aankopen, jongeren vermaken zich vooral op internet. Zowel 18-plussers (70%) als 13-17-jarigen (53%) zijn zeer geïnteresseerd in de risico's die zij daarbij lopen, maar slechts 55% van de volwassenen en 35% van de jongeren is zich van die risico's bewust als ze online zijn. 90% resp. 82% hecht persoonlijk belang aan een goede bescherming. Virussen, hacking, misbruik van financiën en privacy-schendingen en in mindere mate spam en phishing zijn bekend als concrete internet-dreigingen. 57% van de volwassenen heeft zelf te maken gehad met virussen, 34% met oplichting en 15% met phishing. Jongeren kregen naast virussen (63%) en oplichting (28%) te maken met misbruik van wachtwoorden (15%). Ruim 85% gebruikt virusscanners en firewalls, ruim 50% let op bij financiële transacties en bijna 45% is voorzichtig met gegevens. Wat men zelf nog meer kan doen, weten maar weinigen. De meeste burgers zien voor zichzelf wel een belangrijke rol weggelegd bij de bescherming van internet.

Eerste resultaten van de effecten van de campagne geven aan dat het bereik van de campagne zowel onder jongeren als volwassenen hoog is geweest en dat de waardering van de campagne zeer hoog uitpakt. De boodschap, dat je moet opletten welke gegevens je achterlaat om misbruik te voorkomen en wat je daar zelf aan kunt doen is bij velen duidelijk overgekomen. Het is nu aan de Programma's Nationale Veiligheid en Preventie Cybercrime om te bezien wat aan maatregelen en randvoorwaarden nodig en mogelijk is om deze gewaarschuwde burgers nu ook actief te houden.

GOVCERT.NL Cybercrime trendrapport 2009:

Geen verbetering veiligheid internet

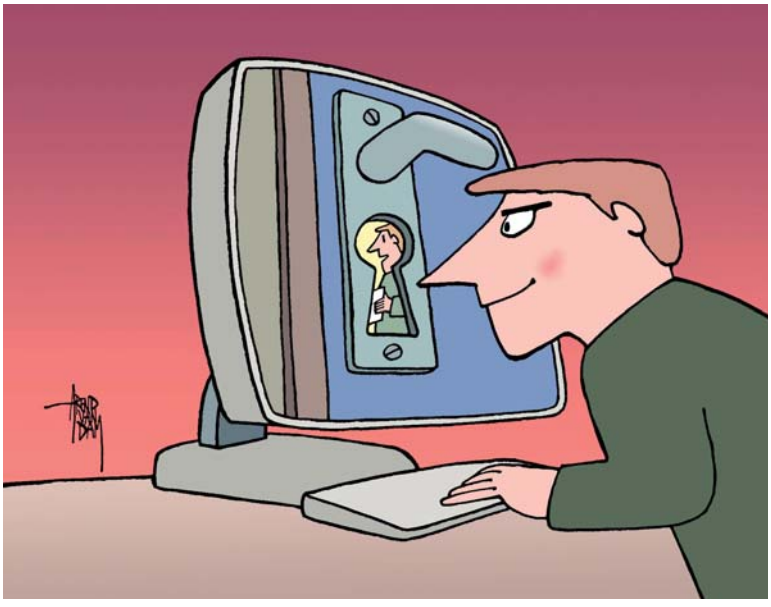
Ton Slewe en Ella Broos
KennisCentrum GOVCERT.NL

In het Trendrapport Cybercrime 2009 van GOVCERT.NL wordt geconstateerd dat het internet er niet veiliger op wordt. Zowel techniek als menselijk gedrag maken dat het internet nog steeds een bijzonder lucratieve werkomgeving voor internetcriminelen is.

Jaarlijks maakt GOVCERT.NL een trendrapport Cybercrime met daarin de belangrijkste ontwikkelingen op het gebied van informatiebeveiliging en cybercrime. Op basis van vertrouwelijke en publieke bronnen en internationale contacten wordt een beeld geschetst van de belangrijkste ontwikkelingen en aan de hand daarvan wordt een analyse gemaakt van de status van het internet én internetcriminaliteit. GOVCERT.NL signaleert acht belangrijke trends, die in dit artikel aan de orde komen.

Kwetsbare eindgebruiker

In het Trendrapport van 2007 signaleerde GOVCERT.NL het al en dit geldt nog steeds: eindgebruikers, zowel thuis als op het werk, blijven een zwakke schakel in internetveiligheid. Zij zijn veelal slachtoffer van internetcriminelen, omdat hun computers met relatief gemak kunnen worden overgenomen. Hierbij wordt misbruik gemaakt van lekken in software en het ontbreken van basisbeveiligingsmaatregelen zoals antivirus software en het tijdig updaten van software. Ook wordt ingespeeld op angst: aanbiedingen van nep-antivirusproducten, waardoor mensen geld kwijtraken en ook hun computer nog wordt besmet. Met deze computers worden botnets gevormd, waarmee op grote schaal criminele activiteiten worden verricht.



Kwetsbare infrastructuur

Steeds duidelijker wordt dat het internet niet is ontworpen voor wat we er vandaag de dag mee doen. De internetprotocollen zijn niet meer afdoende veilig. Het gaat hier om BGP (Border Gateway Protocol), DNS (Domain Name System) en TCP (Transmission Control Protocol). Door de toegenomen afhankelijkheid van het internet, voor zowel bedrijfsleven, overheid als samenleving, moet er met spoed aan gewerkt worden. Dat kan ook, want de beschreven kwetsbaarheden zijn niet nieuw. Voor DNS bijvoorbeeld, is er al ruim tien jaar een veilig alternatief voorhanden. Dit wordt echter heel weinig gebruikt. Ook voor BGP zijn er betere alternatieven, maar die worden langzaam in gebruik genomen. Het probleem is dat de eigenaren van netwerken wel de kosten van aanpassingen dragen, maar er op korte termijn zelf weinig voordeel bij hebben.

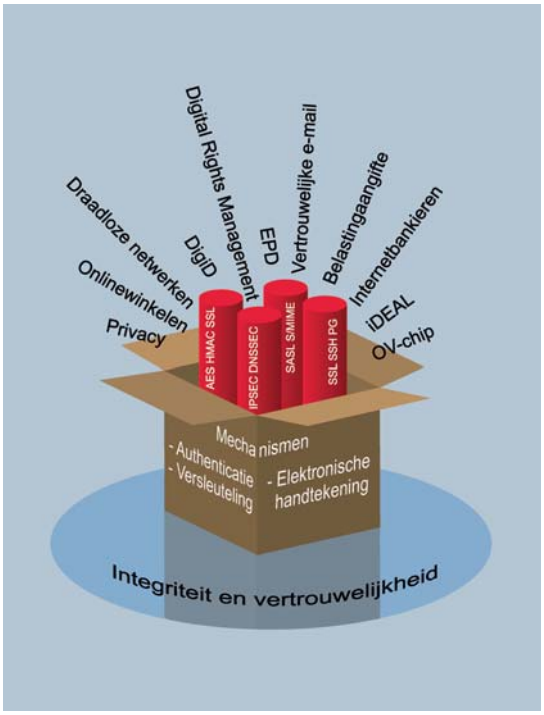
Cryptografie

De basis van informatiebeveiliging is cryptografie. Het is cruciaal voor het garanderen van vertrouwelijkheid en integriteit van informatie en daarmee heel belangrijk voor veel zaken die wij in ons dagelijks leven doen. Cryptografie is niet alleen een wiskundige techniek. Het is een technische oplossing die alleen werkt wanneer deze regelmatig geëvalueerd en goed gebruikt wordt, zowel in technische als in organisatorische zin. Te vaak wordt er op vertrouwd dat een cryptografische techniek die eenmaal goed bevonden is, goed blijft werken. Hierbij wordt er geen rekening mee gehouden dat aanvalstechnieken steeds verbeteren en cryptografische algoritmen dus verouderen. Voorbeelden van verouderde cryptografie zijn MD5, onder andere gebruikt voor het beveiligen van website certificaten en TKIP, gebruikt voor het versleutelen van draadloze netwerken.

Cloud Computing

Meer en meer computertoepassingen verschuiven naar het internet. Deze ontwikkeling wordt 'cloud computing' genoemd: het internet als een wolk waarin allerlei diensten beschikbaar zijn, inclusief virtualisatie, rekenkracht en opslag. Deze diensten bieden groot gebruikersgemak: zelf geen software meer installeren, gegevens altijd en overal kunnen benaderen en goede samenwerkingsmogelijkheden.
De andere kant hiervan is dat er op het gebied van veiligheid het een en ander wordt ingeleverd. Overal beschikbaar betekent ook overal aanvalbaar. Ook schuilt er een risico in de gebruiksvoorwaarden van online diensten. Bijna alle aanbieders houden zich het recht voor de voorwaarden eenzijdig te wijzigen. Sommige voorwaarden bevatten bepalingen waarmee de dienstaanbieder een gebruikslicentie wordt verleend op alle online geplaatste informatie. Hiermee verliest de gebruiker voor een deel de controle over wat er met zijn informatie gebeurt.

Als gevolg van de verschuiving van desktopapplicaties naar webapplicaties, verschuift de aandacht van criminelen van het besturingssysteem naar de browser en de hieraan toegevoegde uitbreidingen.
In het afgelopen jaar zijn er in diverse plug-ins kwetsbaarheden ontdekt en ook misbruikt.



Sociale netwerken als Hyves en MSN zijn actief misbruikt en in het afgelopen jaar doken ook op LinkedIn nepprofielen op waarmee malware werd verspreid. Zelfs Twitter is een geliefd doelwit gebleken van hackers. En daar blijft het niet bij. Internet op de mobiele telefoon wordt steeds populairder. Over het algemeen heeft een mobiele internetter weinig mogelijkheden om zijn mobieltje te configureren. Updaten en veilig houden van software is dus niet zo gemakkelijk.

Deanonimisatie – verlies van privacy

Aan het verlies van privacy zitten twee kanten. Enerzijds maken internetcriminelen steeds meer persoonlijke gegevens buit, bijvoorbeeld door het inzetten van kwaadaardige software of door het omzeilen van de beveiliging van centrale systemen waarin persoonlijke gegevens zij opgeslagen. Anderzijds geven internetgebruikers zichzelf steeds meer bloot door allerlei persoonlijke gegevens op internet achter te laten. Het vervelende voor hen is dat in het internet geen vergeetfunctie is ingebouwd. Internetcriminelen zijn steeds beter in staat de gegevens uit verschillende bronnen, bijvoorbeeld sociale netwerken, te koppelen. Zelf als je op verschillende sociale netwerken verschillende identiteiten hebt, kan deze informatie worden gekoppeld.

GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid. Het werkt aan het voorkomen en afhandelen van ICT-gerelateerde incidenten, 24 uur per dag, 7 dagen in de week. GOVCERT.NL ondersteunt organisaties die een publieke taak uitvoeren, zoals overheidsinstellingen en werken samen met de vitale sectoren. Door middel van www.waarschuwingsdienst.nl wordt het publiek voorgelicht over maatregelen en actuele risico's die betrekking hebben op computer- en internetgebruik.

Kwetsbare software

Kwetsbaarheden in software komen op grote schaal voor. Er moet veel tijd worden besteed aan het up-to-date houden van computers en systemen. Soft- en hardwareleveranciers integreren security vaker in het ontwikkelproces. Ook worden bij software vaker automatische updatemechanismen ingebouwd, zodat het minder moeite kost om updates te installeren.
Ondanks dat staat de ontwikkeling van veilige software nog in de kinderschoenen. Het is vaak toch de verantwoordelijkheid van de gebruiker om veilig te werken en te surfen. Aansprakelijkheid voor fouten in een geleverd product wordt gewoonlijk uitgesloten in het End User License Agreement (EULA), het contract tussen de leverancier en de gebruiker. De Europese Commissie heeft een 'digitale agenda' opgesteld voor de consumentenrechten van morgen. Licentieverlening moet de consument van dezelfde basisrechten garanderen als wanneer hij een product koopt.

Hacktivisme

Geld is de belangrijkste drijfveer van de internetcrimineel. Een andere belangrijke drijfveer is hacktivisme ofwel ideologisch gedreven aanvallen. We zagen aanvallen vanuit Rusland op Estland, en vanuit Rusland op Georgië. Het gaat niet om aanvallen van de Russische overheid, maar door hackers vanuit Rusland. Naast deze cyberoorlogen speelde zich ook een elektronisch conflict af tussen Israël en Hamas. Aanhangers van beide kampen werd opgeroepen malware te installeren waarmee websites van de tegenstander konden worden platgelegd.

Positief

Twee positieve trends die worden gesignaleerd hebben betrekking op samenwerking en opsporing. De samenwerking in de strijd tegen cybercrime wordt steeds hechter én effectiever. Een sprekend voorbeeld is de strijd tegen Conficker, de worm die afgelopen jaar op grote schaal wereldwijd computer heeft geïnfecteerd. Vele partijen uit de hele wereld sloegen de handen ineen om de worm te keren en daardoor zijn de gevolgen van het virus beperkt geweest. Andere voorbeelden zijn te vinden op het gebied van opsporing en berechting. Ook hier is samenwerking en intensief contact tussen onder andere CERT's, ISP's en het Team High Tech Crime van het KLPD en het Openbaar Ministerie uitgemond in succesvolle resultaten. Daarnaast heeft het spamverbod en het toezicht hierop door OPTA grote positieve gevolgen gehad.

Het GOVCERT.NL is trendrapport kan worden gedownload op: www.govcert.nl/trends

Ella Broos, Kenniscentrum, GOVCERT.NL

Samenwerking verstevigd op GOVCERT-symposium

Initiating Change was het thema van het thema van het jaarlijkse ICT-security symposium van GOVCERT.NL op 6 en 7 oktober in Rotterdam. Meer dan 500 gasten uit binnen- en buitenland waren bijeen om kennis te delen, ervaringen uit te wisselen én de samenwerking te versterken.

Op één podium, vrijuit sprekend: de AIVD, het KLPD (National High Tech Crime Unit) het Poolse Computer Emergency Respons Team (CERT-Polska), GOVCERT en Microsoft. Het gaf blijk van de sterke wil om samen te werken tussen overheid, opsporing en marktpartijen als het gaat om de strijd tegen cybercrime. Het delen van operationele, tactische en strategische informatie was het onderwerp, maar ook het samen ontwikkelen van technische tools en zelfs menskracht om nog slagvaardiger te zijn.

Meerwaarde

Want dat, zo stelde onder meer Elly van den Heuvel, general manager van GOVCERT.NL, is waar kansen blijven liggen: “Kijk naar de CERT-community. Op het moment dat er een incident ontstaat, weten we onze operationele informatie heel snel en effectief te delen. Maar het zou goed zijn wanneer we ook andere dingen delen die we gemeen hebben: hoe gaat het in de organisatie, welke projecten kunnen we samen opstarten, wat zijn trends en hoe vinden we goed personeel?” Enkele voorbeelden over de meerwaarde van de uitwisseling van personeel tussen CERT’s passeerden de revue en ook werd besproken hoe de gezamenlijke ontwikkeling van de Honey SpiderProject (door CERT-Polska, SurfNet en GOVCERT.NL) een voorbeeld is van het bouwen van tools die door de hele gemeenschap kunnen worden gebruikt.

Veertig sessies

Onder de sprekers tijdens het symposium bevonden zich grote namen uit de internet-security-wereld. Bruce Schneier van BT-Counterpane, Mikko Hyppönen van F-Secure, David Rice van de Monterey Group en Andy Purdy van de George Mason University gaven hun eigen kijk op ICT-security en alle aspecten die daar komen kijken. Staatssecretaris Ank Bijleveld opende de tweede dag met een beschouwing over de veiligheid van overheidsorganisaties en de manier waarop die verbeterd kan worden. In de circa veertig parallelsessies verspreid over twee dagen, spraken experts over onder meer techniek, opsporing, dreigingen en maatschappelijke impact.

Tien CERT’s

Tijdens de afsluiting van het symposium constateerde Van den Heuvel:”Een aantal stappen is gemaakt. We hebben een recordaantal mensen uit de beleidsdirecties van diverse ministeries gehad, wat betekent dat ook voor hen het programma aansprekend is gebleken. Daarna zijn er met de hoofden van CERT’s uit tien landen afspraken gemaakt over intensievere samenwerking en kennisdeling. De staatssecretaris van BZK heeft nog eens onderstreept hoe belangrijk het onderwerp is voor de overheid. Ik geloof dat we een forse stap hebben gemaakt in deze twee dagen. Volgend jaar zullen we kijken hoe de voortgang is op deze drie onderwerpen.”

Pim Takkenberg,
wnd. teamleider HTC, Dienst Nationale Recherche, KLPD

Het werk van het Team High Tech Crime van de Dienst Nationale Recherche haalt met enige regelmaat de krantekoppen. Zo is in maart j.l. een 22-jarige man uit Breda aangehouden die wordt verdacht van het saboteren van websites, waaronder die van geenstijl.nl. Voor het saboteren van de website gebruikte hij vermoedelijk een botnet. Dat is een netwerk van duizende 'gekaapte' computers.

Team High Tech Crime

"Sporen verdampen waar je bij staat"

Nationale Recherche

Het Team High Tech Crime bestaat uit dertig mensen, verspreid over twee onderzoeksgroepen. Een onderzoeksgroep bestaat uit tactische rechercheurs en digitale adviseurs; een relatief jong team met een hoog opleidingsniveau. Het team is 24 uur per dag, zeven dagen in de week bereikbaar en vormt het contactpunt cybercrime voor partners overal ter wereld. De onderzoeken van het team zijn 'level drie' cybercrime-zaken. Deze vorm van criminaliteit betitelen we als High Tech Crime. Het gaat met name om cybercriminaliteit gericht tegen ICT-infrastructuren. We moeten continu afwegingen maken welke zaken we behandelen. We kunnen nou eenmaal niet alles doen. Daarom richten we ons op zaken die een grote invloed of impact op onze samenleving hebben en vooral op georganiseerde cybercrimenetwerken.

Internationale samenwerking

Internet houdt niet op bij de landsgrenzen. Onderzoeken naar high tech crime zijn overwegend internationaal. Het team HTC werkt daarom samen met internationale organisaties zoals de Amerikaanse FBI, de Engelse SOCA, Russiche FSB, Oekraïense SBU en de Australische High Tech Crime Unit. We willen dat al deze landen een top tien/twintig van hun belangrijkste cybercriminelen opstellen. Deze lijsten leggen we naast elkaar en dan bekijken we wie er welke gegevens tegen welke criminelen heeft. Op die manier kunnen we internationale criminele netwerken in kaart brengen en de beste aanpak voor de bestrijding van cybercrime formuleren. We willen Nederland zo onaantrekkelijk mogelijk te maken voor high tech dreigingen uit alle hoeken van de wereld. In de internationale samenwerking nemen wij bewust een voortrekkerspositie in. Rechtshulpverzoeken behandelen we bijvoorbeeld in een tijdsbestek van uren, eerder dan dagen. We willen daarmee niet alleen een voorbeeld geven aan andere landen, maar ook ervoor zorgen dat zij óns sneller helpen. Informatie moeten we vlug kunnen uitwisselen en digitale sporen snel veiligstellen, want ze verdampen waar je bij staat. Gegevens op een server kunnen met een druk op de knop verplaatst of verwijderd worden. Daarom moeten we kunnen optreden op het moment dat de crimineel de server nog gebruikt.

Leren

In de beginfase werkte het Team HTC zaakgericht, maar in de vluchtige wereld van de cybercriminaliteit werkte dat niet optimaal. De ervaring leerde ons dat we beter dadergericht konden werken. De belangrijkste reden is gelegen in het werken in de actualiteit. Vaak dienen zaken zich pas aan, enige tijd nadat zij hebben plaatsgevonden. Veel sporen zijn dan verdwenen en daarmee is de kans op oplossing verkleind. Omdat de digitale wereld zo veranderlijk is, moeten we telkens goed kijken welke aanknopingspunten kansrijk zijn en afwegen wat te onderzoeken. In onze onderzoeken werken we regelmatig samen met andere diensten en team van het KLPD, zoals de Dienst Specialistische Recherchetoepassingen en het Team Digitale Expertise van onze eigen Dienst Nationale Recherche. Zij hebben diepte-expertise over onderwerpen die we kunnen inzetten. We hoeven niet alle specialistische kennis zelf in het team te hebben.

Cybercrime versus high tech crime
Er is verschil tussen cybercrime en high tech crime. Cybercrime is criminaliteit waarbij computers, mobiele telefoons en andere vormen van geavanceerde technologie betrokken zijn. High tech crime is cybercrime in zware en georganiseerde vorm, die grote impact heeft op onze samenleving. De Dienst Nationale Recherche is onderdeel van het Korps landelijke politiediensten.

De airbags van de PC

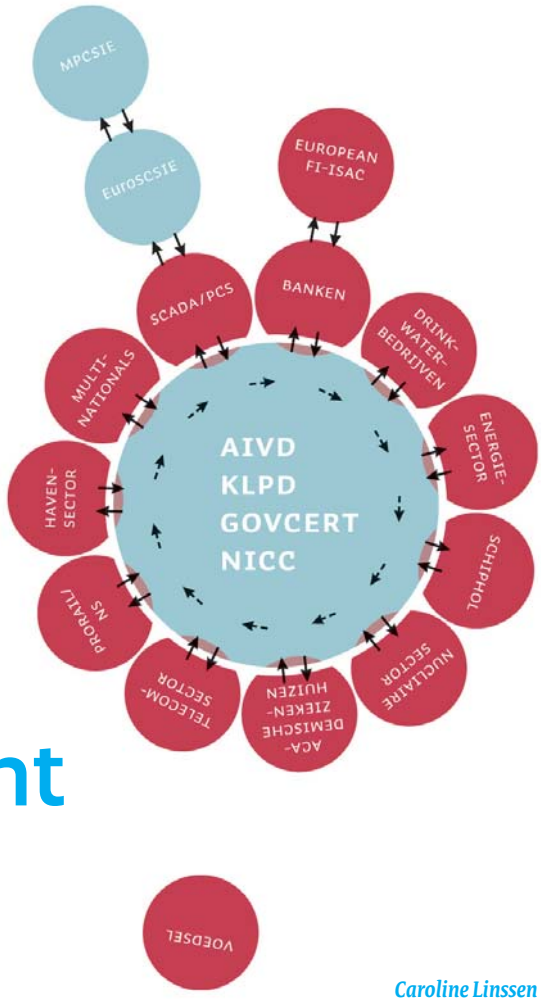
ir. M.J.A. Tuinder,
hoofd business unit Nationaal Bureau voor Verbindingsbeveiliging, Algemene Inlichtingen- en Veiligheidsdienst

In 1896 worden de eerste commerciële auto's verkocht. Deze zijn zeer onbetrouwbaar. Ze worden zelfs geleverd met een reparatiekit voor de bestuurder. Auto's zijn daarnaast gevaarlijk en duur in gebruik. Dat is geen probleem omdat ze meer als gadget gezien worden dan als een vervoermiddel. Bij ongelukken vallen veel doden en gewonden. Dit leidt al snel tot wetgeving om vooral de overige verkeersgebruikers te beschermen. Maar er worden pas in 1975, nadat de auto onmisbaar in ons leven is geworden, passende eisen gesteld aan de veiligheid van de inzittenden, onder meer door verplichtstelling van de veiligheidgordel. Er volgen meer nieuwe beschermingsmaatregelen als airbags, goede testmethodieken voor de veiligheid (als de elandtest), certificering (zoals de Euro NCAP sterren) en keuringen om de weg op te mogen (bijvoorbeeld de APK). Hierdoor zijn de verantwoordelijkheden duidelijker belegd. Ook is een onderlinge vergelijking van geboden veiligheid tussen autotypes mogelijk, waardoor deze kan worden meegenomen in de aankoopbeslissing. Na de falende elandtest is het nooit meer iets geworden met de verkoop van de Baby-Benz.

De eerste commerciële computers zijn zeer onderhoudsintensief. Personeel werkt in ploegendiensten om de computer in bedrijf te houden. Met de komst van de 'Personal Computer' (PC) in 1980 ontdekt de zakelijke markt de mogelijkheden om bedrijfsprocessen te verbeteren en versnellen. De noodzakelijke programmatuur wordt geleverd met een 'beperkte verantwoordelijkheid': de makers garanderen niet dat je mag vertrouwen op de programmatuur. En terecht, zo blijkt. Met de komst van de thuiscomputer ontdekken hackers volop mogelijkheden om onvolkomenheden in computersoftware te misbruiken. Met de komst van internet, rond 1987, ook om computers van andere mensen te misbruiken. Tegelijk met de toenemende populariteit van internet, vanaf 1994, professionaliseert de hacker en ontstaat internetcriminaliteit. De software-industrie ontwikkelt ondertussen steeds betere methoden voor de verspreiding van lapmiddelen, zogenaamde 'patches'. Dat zijn reparatieprogramma's waarmee gebruikers bekende onvolkomenheden in hun software kunnen repareren. Terwijl bijna alle bedrijfsprocessen afhankelijk zijn van computers, blijken softwaremakers nog steeds niet in staat de kwaliteit van hun producten te garanderen. Sterker nog, sommige softwaremakers zien zich bijna maandelijks gedwongen om lapmiddelen aan te bieden zodat klanten zelf in staat zijn fouten in afgenomen producten te herstellen. Ondertussen brengen de gebruikers defecte software niet boos naar de winkel terug.

De automobiel en de computer. Twee onmisbare zaken die een vergelijkbare ontwikkeling doormaken. De auto is tegenwoordig behoorlijk betrouwbaar, de computer nog niet. Als we de ontwikkeling van de veiligheid van auto's spiegelen aan de computer, zou het nog wel eens tientallen jaren kunnen duren voordat iedereen zonder nadenken en inspanning op zijn computer mag vertrouwen. De airbag van de computerbeveiliging bestaat nog niet, maar gelukkig zijn er wel positieve ontwikkelingen. Er zijn ISO-standaarden vastgesteld voor de inrichting van een veilige informatievoorziening, de "Common Criteria" worden internationaal steeds beter erkend als standaard voor de beoordeling van beveiligingsfunctionaliteit en er bestaan door de AIVD nationaal goedgekeurde producten voor de beveiliging van onze meest vertrouwelijke informatie. Zo zijn met een beetje moeite en hulp van anderen de risico's nog enigszins te beperken. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD levert een actieve bijdrage aan de nationale veiligheid door deze risico's voor informatiebeveiliging van cruciale informatie in kaart te brengen en waar mogelijk te beperken. Veilig informatieverkeer komt zo gaandeweg dichterbij.

Het mooiste resultaat van vier jaar NICC is het opgebouwde publiekprivate netwerk in het Informatieknooppunt Cybercrime. Programmamanager Annemarie Zielstra: “Als er een belangrijk onderwerp opkomt, heb je alle partijen snel bij elkaar om slagvaardig te reageren. Voorheen zou je daar maanden over doen.” Het programma heeft zijn belangrijkste doelstelling bereikt. Binnenkort wordt bekend hoe dat resultaat geborgd gaat worden.



“Voortzetting **Informatieknooppunt Cybercrime** is mooi compliment”

Caroline Linssen

In 2006 was er nog geen structureel publiekprivaat overleg om kennis en informatie over cybersecurity uit te wisselen. Het NICC ontwikkelde daarvoor de Nationale Infrastructuur ter bestrijding van Cybercrime. Het Informatieknooppunt Cybercrime, één van de vele NICC-projecten, groeide uit tot het kloppend hart van de Nationale Infrastructuur. Er zijn tien (vitale) sectoren op aangesloten, van de bancaire sector en energie- en waterleidingbedrijven tot transport en telecom. AIVD, KLPD, GOVCERT.NL zitten bij alle overleggen aan tafel, het NICC is facilitator en intermediair. Auke Huistra, projectmanager Informatie-knooppunt: “Je krijgt steeds meer inter-sectorale thema’s zoals Process Control Security en Outsourcing. Ook koppelen we mensen aan elkaar. Zo zocht een deelnemer aan het Multinationals-overleg informatie over de inrichting van Risk Management. Dan brengen we hem in contact met iemand uit het bancaire overleg, want banken hebben daar ervaring mee.”

Korte lijnen

Het succes van het NICC zit in de werkwijze. Huistra: “Het kleine kernteam houdt de lijnen kort en dwingt te focussen op dingen waar je goed in bent. Daaromheen verzamelden we een pool van experts van TNO, universiteiten en consultancy-bureaus, die ook onze ambassadeurs in het veld zijn.” Het wendbare team speelt snel in op nieuwe ontwikkelingen. “Daar rollen publiekprivate initiatieven uit als de nationale ‘Roadmap to secure Process Control Systems’, waarmee je cybersecurity breder trekt.”
Initiatieven zonder energie worden snel verlaten ten gunste van projecten waar wel de vaart in zit. Annemarie Zielstra: “De publiek-private partijen moeten er wat aan hebben. Dus niet als de zoveelste club er weer wat bij gaan verzinnen, maar aansluiten bij zaken waar partijen zelf mee bezig zijn.”
Het NICC groeide snel uit tot makel- en schakelpunt dat partijen bij elkaar brengt. “We steken veel tijd en energie in het leggen van contacten en het opbouwen van vertrouwensrelaties. Onze onderzoeks-rapporten verdwijnen niet in een la, maar zijn juist het begin van nieuwe activiteiten. Toen we de Nationale Infrastructuur op orde hadden, bleek dat we ons ook op inter-nationale samenwerking moesten richten. Cybercrime stoort zich niet aan landsgren-zen. Dus zitten we nu in internationale gremia, op zoek naar samenwerkingspartners, good practices en expertise. Onze aanpak van het Informatieknooppunt wordt in andere landen gebruikt als voorbeeld.”

Informatieknooppunt Cybercrime gaat door

Het programma NICC loopt ten einde. Binnenkort wordt besloten hoe het Informatieknooppunt geborgd wordt. De werkwijze van het NICC staat niet ter discussie: zonder deze facilitator zou het opgebouwde netwerk in elkaar zakken. Huistra: “We zijn blij met de uitspraak van plaatsvervangend directeur Hellen van Dongen van de Directie Telecommarkt: het Informatieknooppunt Cybercrime is een succesformule en gaat door.”
“Onze manier van werken wordt gewaardeerd”, constateert Zielstra. “Dat blijkt uit de evaluatie van het Informatie-knooppunt. We wisten bij de start niet dat het Informatieknooppunt zo belangrijk zou worden. Dat het structureel wordt voortgezet, is een mooi compliment aan alle publieke en private partijen die het tot een succes hebben gemaakt.”

NAVI en cybersecurity

Kim Veenendaal,
communicatieadviseur NAVI

Het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) brengt overheid en bedrijfsleven samen om te werken aan de verbetering van de bescherming van vitale infrastructuur in Nederland tegen moedwillig menselijk handelen. Deze bescherming heet security. De activiteiten van het NAVI zijn gericht op fysieke, personele, organisatorische en digitale dreigingen.

Beheerders en eigenaren van de vitale infrastructuur worden door het NAVI ondersteunt met een platform voor informatie-uitwisseling, kennis & expertise en een (inter)nationaal contactpunt.

Het NAVI faciliteert onder meer bijeenkomsten, kennis- en informatie-knooppunten en verschillende uitvoerings-programma's. Daarnaast participeert het NAVI in bijvoorbeeld onderzoekstrajecten en risicoanalyses. Enkele voorbeelden zijn de SOVI quickscan van afhankelijkheden en kwetsbaarheden van ICT binnen vitale sectoren, het project en de ondersteuning bij de implementatie van security management systemen Capaciteiten Analyse Energie en Telecom (CAET) binnen de olie- en petrochemische sector.

Binnen de Telecom/ICT sector zijn naast het NAVI tevens andere organisaties actief binnen hun eigen taken en bevoegdheden. Ten aanzien van vitale infrastructuur werkt het NAVI daarom nauw samen met organisaties zoals de AIVD, het NCTb, het KLPD, TNO en specifiek voor ICT, met GOVCERT.NL. In deze samenwerkingen wordt kennis en ervaring uitgewisseld en worden gezamenlijke activiteiten ontplooid. De Nationale Infrastructuur Cyber Crime (NICC) faciliteert de informatieknooppunten op het gebied van ICT met betrekking tot cyber crime en process control security.

veiligheid en veerkracht

Cyber Security

in cyberspace

Tom Orton,
Office of Cyber Security, Cabinet Office, United Kingdom

Toenemende afhankelijkheid

De *Digital Britain*-strategie van de overheid toont overduidelijk aan hoe belangrijk internet en netwerken (verder in dit artikel gemakshalve aangeduid als "cyberspace") zijn voor onze natie. Alleen al de 50 biljoen Britse pond die per jaar online omgaan onder consumenten illustreert hoezeer onze nationale welvaart afhangt van de nieuwe technologie van cyberspace. Cyberspace is steeds vaker het platform voor de activiteiten van de overheid en organisaties in alle sectoren, maar ook voor individuele burgers, die het internet gebruiken voor bijvoorbeeld online bankieren, het onderhouden van sociale contacten en aankopen. Deze digitale netwerkactiviteiten bieden een overweldigend scala aan voordelen en kansen, dus moeten we ervoor zorgen dat het Verenigd Koninkrijk in de positie blijft daarvan te profiteren. We moeten ons echter realiseren dat er afgezet tegen de kansen ook een aantal reële en snel groeiende bedreigingen mee gemoeid zijn: er zijn nu eenmaal mensen die ons via cyberspace kwaad willen berokkenen. Bovendien is cyberspace vanwege de snelle technologische ontwikkelingen en veranderende gebruikspatronen een dynamische omgeving vol uitdagingen waarmee we gelijke tred moeten zien te houden. Precies om die reden hebben we een Cyber Security-strategie uitgewerkt waarin staat wat de regering doet om nu en in de toekomst te waarborgen dat we de risico's minimaliseren en optimaal profiteren van kansen.

Toenemende bedreigingen

Vanwege de lage kosten en zijn anonieme karakter oefent cyberspace een grote aantrekkingskracht uit op lieden met weinig goeds in de zin. De laagdrempeligheid gecombineerd met de problemen met detectie en opsporing maken dat ook de georganiseerde criminaliteit, vijandige staten en terroristen naar believen gebruik kunnen maken van cyberspace. We moeten ons er zeer nadrukkelijk van bewust zijn dat er allerlei personen zijn met intenties en vaardigheden die een concrete bedreiging vormen voor onze veiligheid en welvaart. Burgers denken vaak aan geavanceerde cyberspionage onder leiding van de staat, en ook dat is natuurlijk een serieuze zaak, maar we moeten ons ook realiseren dat criminelen misbruik blijven maken van de kwetsbare plekken in de IT-systemen van overheid, bedrijfsleven en burgers en daarvoor over allerlei middelen en technieken beschikken, variërend van phishing tot malware. Online fraude veroorzaakt niet alleen financiële schade, maar gaat ook ten koste van het vertrouwen van het publiek in het internet. We moeten dus alert zijn op aanvallen op overheidssystemen, onze vitale infrastructuur, op burgers en het bedrijfsleven en ze zien te voorkomen.

Wat er nu gebeurt

Het feit dat we een nieuwe strategie publiceren laat onverlet dat we al heel veel energie, middelen en expertise hebben gestoken in de cyberveiligheid van het Verenigd Koninkrijk. Het probleem is immers niet nieuw. De overheid neemt al jaren op allerlei fronten maatregelen om de cyberveiligheid te waarborgen. De National Information Assurance Strategy uit 2003 was bijvoorbeeld gericht op de eerste maatregelen om de integriteit, beschikbaarheid en veiligheid van informatie- en communicatiesystemen en de informatie die erin omgaat te waarborgen; de Cyber Security-strategie bouwt hierop voort. Er gebeurt dus al heel veel om het

Verenigd Koninkrijk – zowel binnen de overheid als in samenwerking met het bedrijfsleven en andere sectoren – te beschermen tegen bedreigingen via cyberspace.

Het Britse ministerie van Binnenlandse Zaken, de Serious Organised Crime Agency en de politie houden zich allemaal bezig met het bestrijden van criminele activiteiten in cyberspace. Recente initiatieven hebben geleid tot de oprichting van nieuwe eenheden ter bestrijding van online criminaliteit, zoals het Child Exploitation and Online Protection Centre en de Police Central e-crime Unit. In juni heeft de Association of Chief Police Officers een e-crimestrategie gepubliceerd die de basis zal vormen voor een consistentere aanpak door de vaardigheden en capaciteit uit te breiden en cybercriminaliteit centraler te stellen bij het politiewerk en de handhaving.

Het CPNI (Centre for the Protection of National Infrastructure) adviseert bedrijven en organisaties die deel uitmaken van de vitale infrastructuur van het Verenigd Koninkrijk over de veiligheidsmaatregelen die ze kunnen nemen. Het betreft de volgende sectoren waar vitale diensten verleend worden: energie, voedsel, water, transport, communicatie, overheid en publieke diensten, noodhulpdiensten, gezondheidszorg en de financiële sector. Het CPNI beschikt ook over een Computer Emergency Response Team (CERT) dat reageert op meldingen van aanvallen op netwerken in de particuliere sector.
Alle ministeries en overheidsinstanties hebben toegang tot het GSI (Government Secure Intranet), een netwerk van beveiligde verbindingen tussen ongeveer 200 departementen en instanties, CESG, een deel van GCHQ en de National Technical Authority for Information Assurance. Hier wordt ministeries geadviseerd hoe ze cyberaanvallen kunnen detecteren, de gevolgen ervan kunnen beperken en hoe ze zich ertegen kunnen beschermen. CESG beheert het GovCertUK waarmee waarschuwingen en alarmen worden afgegeven en bijstand wordt verleend voor het verhelpen van ernstige IT-incidenten in de publieke sector.

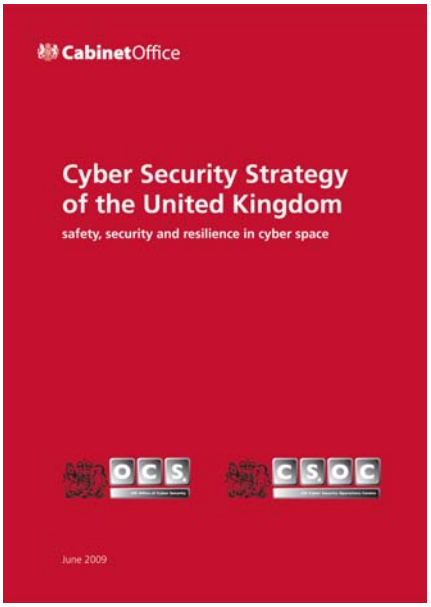
Gedeelde verantwoordelijkheid

Alle gebruikers van cyberspace moeten bijdragen aan de veiligheid ervan. Het is aan de overheid en het bedrijfsleven samen te werken om veiliger producten en diensten te leveren, hun informatiesystemen veilig te beheren en de privacy van burgers te beschermen. Ook individuele burgers dienen eenvoudige beveiligingsmaatregelen te nemen om zichzelf, hun gezinnen en anderen in de maatschappij te beschermen. Denk bij voorbeeld aan een onbeveiligde PC die besmet is met malware, deel uitmaakt van een botnet en gebruikt wordt voor aanvallen op institutionele doelwitten: exemplarisch voor de manier waarop netwerkaanvallen vaak verlopen. Dit illustreert hoe belangrijk het is dat iedereen beseft dat de veiligheid van het internet staat of valt met een gezamenlijke aanpak. Daarom ondersteunt de overheid het publiek/private Get Safe Online-initiatief om de bewustwording onder het publiek en het midden- en kleinbedrijf te bevorderen.

Volgende stappen

De nieuwe strategie helpt bij de bescherming van het Verenigd Koninkrijk. Het bouwt voort op de activiteiten die reeds ontplooid zijn, identificeert de lacunes en

GET SAFE ONLINE .org TM



overlap in werkterreinen en resulteert in twee nieuwe organisaties voor het ontwerpen, initiëren en monitoren van een werkprogramma om die lacunes en overlap aan te pakken. De Cyber Security-strategie biedt het strategische kader om daarbij systematisch te werk te gaan met de focus op duidelijke doelstellingen op hoog niveau: terugdringen van de risico's van het gebruik van cyberspace in het Verenigd Koninkrijk; gebruikmaken van de kansen die cyberspace biedt; dit alles wordt mogelijk gemaakt door de benodigde kennis, vaardigheden en besluitvorming te verbeteren. In de strategie wordt ook expliciet benadrukt dat er ethische normen moeten worden gehandhaafd: mensen maken zich terecht zorgen om het behoud van hun burgerrechten en met name over de bescherming van hun persoonlijke privacy. Bij de lancering van de strategie werd benadrukt dat de inzet van de bevoegdheden van de overheid, net als bij alle overige kwesties op het gebied van de nationale veiligheid, proportioneel moet zijn en verenigbaar met de persoonlijke vrijheid. Het Verenigd Koninkrijk is voornemens een adviesgroep voor ethische kwesties op te zetten om de nodige inzichten te verkrijgen voor de activiteiten ter wille van de cyberveiligheid.

Ten einde de doelstellingen van de strategie te bewerkstelligen is een Office of Cyber Security in het leven geroepen dat belast wordt met de strategische leiding binnen de gehele overheid. Ook is er een multi-institutioneel Cyber Security Operations Centre in Cheltenham opgericht voor de actieve monitoring van het internet en de coördinatie bij incidenten, waardoor we een beter inzicht krijgen in de aanvallen op Britse netwerken en betere adviezen en informatie kunnen verschaffen over de risico's voor burgers en bedrijfsleven. Er is sinds de publicatie van de strategie al veel vooruitgang geboekt. De kopstukken van de nieuwe organisaties zijn benoemd en zij zijn hard bezig om personeel te werven binnen de overheid. Ondertussen wordt ook hard gewerkt aan de prioriteitsgebieden die in de strategie als buitengewoon urgent zijn aangemerkt.

Beide organisaties streven ernaar al in het najaar van 2009 over voldoende mensen en middelen te beschikken om de eerste resultaten af te leveren. Een van de eerste prioriteiten is de Cyber Security Industrial Strategy waarmee alle manieren waarop het bedrijfsleven en de overheid op dit gebied met elkaar te maken hebben in kaart worden gebracht, variërend van de inkoop tot de regelgeving. Zodra dat afgerond is en ook andere terreinen van het bedrijfsleven zijn geanalyseerd, wordt onderzocht hoe ze kunnen worden geoptimaliseerd om tegemoet te komen aan de behoeften van bedrijfsleven en overheid. Ook blijven we ons richten op de e-criminaliteit om de beste structuur te creëren voor nauwe samenwerking tussen SOCA, de gemeentepolitie en andere betrokkenen om de bedreigingen aan te pakken. Het Verenigd Koninkrijk is goed vertegenwoordigd in alle relevante internationale fora waar het internet steeds vaker op de agenda staat. We zetten intensieve samenwerkingsverbanden op met gelijkgestemde landen. Tot slot verdiepen we ons in de doctrine waarop cyberveiligheid gebaseerd is – een nieuw terrein dat zorgvuldige planning vereist.

Transnationale samenwerking voor een transnationaal probleem

Cyberspace is per definitie transnationaal. Cybercriminelen trekken zich niets aan van nationale grenzen en proberen er juist van te profiteren. De noodzaak van internationale coördinatie op het gebied van cyberveiligheid met bondgenoten spreekt dan ook voor zich. Er bestaan al nauwe relaties tussen Britse overheidsorganisaties die belast zijn met de cyberveiligheid en hun counterparts in het buitenland. Nu moeten we op deze relaties voortbouwen, de coherentie vergroten en nieuwe betrekkingen aanknopen waar we lacunes aantreffen. Het OCS neemt het voortouw bij de internationale inspanningen van het Verenigd Koninkrijk op het gebied van cyberveiligheid en coördineert de formulering en presentatie van de kernboodschappen van het Verenigd Koninkrijk in de belangrijkste fora. Dit draagt bij aan de coherentie van zijn activiteiten met buitenlandse partners en internationale organisaties. In het kader daarvan blijven we zoeken naar gelegenheden voor overleg met onze belangrijkste bilaterale partners, met name de Verenigde Staten, om ideeën en ervaringen uit te wisselen.

Conclusie

We moeten onze positie in cyberspace veiligstellen zodat burgers en bedrijfsleven er met vertrouwen gebruik van kunnen blijven maken. Er valt veel te doen en we onderschatten de omvang van hetgeen voor ons ligt dan ook geenszins. Met de publicatie van de strategie hebben we concreet vooruitgang geboekt en een solide basis gelegd. Daar moeten we aan vasthouden en zorgen dat ze wordt waargemaakt.

Jan Willem van Borselen,
coördinerend senior beleidsmedewerker, directie Nationale Veiligheid, ministerie van BZK

Weerbaarheid van elektronische telecommunicatie

Op 4 en 5 november werd door het Zweedse Post en Telecom agentschap (PTS) een internationale conferentie gehouden over "resilient electronic communications". Doel was publieke en private organisaties ervaringen te laten uitwisselen over de uitdagingen die het creëren van een robuuste en veilige informatie-maatschappij met zich meebrengt.

Er liggen twee voorstellen van de Europese Commissie in relatie tot de weerbaarheid van telecommunicatie. Het zogenaamde Telecom Package tot herziening van de wettelijke kaders en het voorstel om de bescherming van de vitale informatie infrastructuur (CIIP) te verbeteren. Er lopen discussies over de vraag hoe overheden en bedrijven in PPS verband het beste kunnen samenwerken. Een aantal lidstaten, waaronder Nederland, heeft Computer Emergency Respons Teams (CERT's) ingesteld, andere landen hebben plannen deze op te richten.

Op 9 en 10 november is in Visby (Zweden) een EU conferentie georganiseerd om te komen tot een strategische ICT beleidsagenda voor 2015 die bijdraagt aan een groene kenniseconomie. In 2010 stelt de Commissie de agenda voor 2015 vast.

DG Treschow (PTS) legde de verbinding tussen weerbaarheid, het belang van (persoonlijke) netwerken en informatie-beveiliging. De CERT's vervullen een belangrijke rol en alleen door samenwerking kunnen nieuwe stappen worden gezet. Vervolgens meldde de Zweedse minister voor infrastructuur dat alle lidstaten hebben ingestemd met nieuwe regelgeving voor het Telecom pakket! Ontwikkelingen als cloud computing brengen privacy issues met zich mee waarvoor beschermende maatregelen noodzakelijk zijn. Concrete voorstellen worden gepresenteerd op de Telecom Council in december. Om PPS beter te maken is onderling vertrouwen nodig en het uitdragen van goede samenwerkings-voorbeelden. Niet alleen ICT – maar ook andere daarmee verbonden infrastructuren zoals transport – (hogesnelheidstreinen) en energiesystemen (windmolenparken) moeten worden beoordeeld op hun weerbaarheid tegen uitval. De ICT afhankelijkheid van elektriciteit vereist maatregelen om te voorkomen dat de werking van vitale infrastructuren en informatiesystemen van een enkel telefoontje (kunnen) afhangen. Netwerken moeten van zichzelf robuust zijn. Doordat systemen voortdurend veranderen en aan elkaar worden gekoppeld vergt dat ook nieuwe communicatie strategieën.

Uit een Noorse oefening in 2008 met gesimuleerde cyberattacks en plotselinge stroomuitval bleek dat er meer dan de verwachte afhankelijkheden en verstoringen ontstonden. De noodzaak van intersectorale coördinatie bleek groot en een snelle coördinatie lastig. Wezenlijk is vooraf het netwerk goed op orde te hebben. De NATCERT vervult een cruciale functie maar bleek geen toegang te hebben tot systemen waarmee IP adressen van het internet konden worden gehaald. Snelle informatie-uitwisseling is essentieel voor vroegtijdige alertering. Er ontstond een conflict tussen de belangen van handhavers en het belang van operationele continuïteit. Weinig partijen zijn zich echt bewust van hun afhankelijkheid van het internet. ICT is een doorsnijdend thema waardoor er geen duidelijk eerstverantwoordelijk ministerie is aan te wijzen dat de leiding neemt bij een ICT crisis.

Jenna Menna (DHS) gaf een toelichting op de Amerikaanse oefening Cyberstorm III (najaar 2010). Gezamenlijk oefenen verhoogt de weerbaarheid, laat de witte vlekken zien tussen beleid en handhaving en stimuleert besluitvormers tot verbeteringen. Respons-plannen worden getest. Bij Cyberstorm III zijn vele sectoren betrokken en spelen de CERT's en defensiespecialisten een cruciale rol. Er wordt gewerkt aan een National Cybersecurity Communications Center.

Om de weerbaarheid de komende jaren te versterken moeten inspanningen gericht zijn op: het versterken van het security netwerk, het maken van een gezamenlijke strategische security agenda in EU verband, het identificeren van de belangrijkste uitdagingen, een hybride aanpak van security/cert en handhaving, het vinden van een balans tussen werken aan een weerbaar en robuust netwerk en economische belangen, omgang met het paradigma dat informatiebeveiliging het maatschappelijke leven mogelijk maakt c.q. verbetert en anticiperen op nieuwe trends en ontwikkelingen. Samengevat: een nuttige conferentie wat ambities betreft: uitdagingen zijn er genoeg, de komende tijd zal laten zien wat het resultaat is van die inspanningen!

Meer info:
www.pts.se/english
www.eu2009.pts.se
www.ourvisbyagenda.eu/
www.enisa.europa.eu
www.dhs.gov/index.shtm

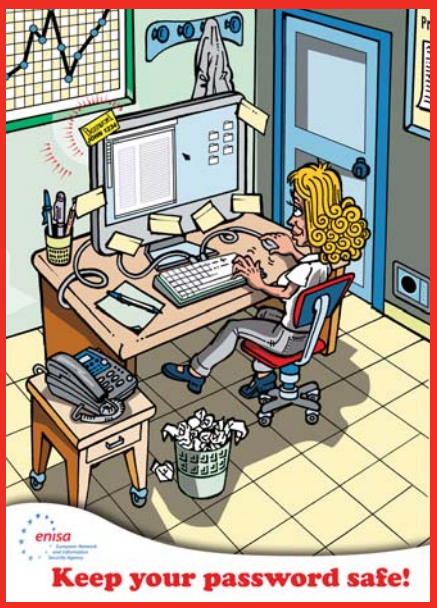
Hans Oude Alink,
ministerie van Economische Zaken

Cybersecurity

Informatie- en communicatietechnologieën en diensten zijn steeds meer met onze dagelijkse activiteiten vervlochten. Sommige daarvan vormen een vitaal onderdeel van de economie en maatschappij: ze verschaffen essentiële goederen en diensten of vormen het ondersteunende platform van andere vitale infrastructuren. Verstoring of vernietiging ervan hebben een ernstige impact op vitale maatschappelijke functies. Het Economisch Wereldforum schatte in 2008 de kans op een grote ICT-verstoring, die de mondiale economie zo'n 250 miljard Amerikaanse dollar kan kosten, in de volgende 10 jaar op 10 à 20%.
ICT kent geen grenzen en dus gaat ook allerlei digitaal ongerief, zoals spam en virussen tot en met grote digitale aanvallen, over de internationale snelwegen van het Internet.
Daarom heeft ook de Europese Unie de bescherming van de vitale Telecom/ICT opgepakt. Zij gebruikt hiervoor de term Vitale Informatie Infrastructuur, oftewel Critical Information Infrastructure Protection (CIIP).

Voorgeschiedenis van CIIP
Vanaf de beginjaren van deze eeuw wijst de Europese Commissie op de noodzaak van afstemming van de verschillende inspanningen om in de samenleving vertrouwen te wekken in elektronische communicatie en diensten. In 2007 heeft de Europese Raad hiervoor een Resolutie voor een veilige informatiemaatschappij aangenomen. Deze resolutie ging o.m. in op beveiliging en weerbaarheid van ICT-infrastructuren.
Daarnaast is in 2004 een Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) opgericht. Dit agentschap heeft tot doel binnen de EU een hoog niveau van netwerk- en informatiebeveiliging te realiseren.
Verder is van belang dat in het kader van het Europees programma voor de bescherming van vitale infrastructuur (EPCIP) in 2008 een Richtlijn is uitgebracht[1]. Deze richtlijn beoogt de identificatie van zogenaamde Europese vitale infrastructuren te realiseren en de beoordeling van de noodzaak om de bescherming van dergelijke infrastructuren te verbeteren. De ICT-sector is een van de sectoren die in dit programma zullen worden onderzocht vanaf 2011.
Een volgende stap is het aanbrengen van meer concrete inhoud aan het begrip weerbaarheid van Vitale Informatie Infrastructuren binnen de EU. De Europese

[1] 2008/114/EG d.d. 8 december 2008



in de **Europese Unie**

Commissie heeft dit in de vorm van een Mededeling opgepakt.

Mededeling betreffende de bescherming van vitale informatie infrastructuren[2]
De mededeling is een door Commissie opgesteld document om de discussie over CIIP binnen de Unie verder te verdiepen en richting te geven aan een aantal concrete acties.
Deze komen voort uit de constatering dat er nog teveel ongelijke en ongecoördineerde nationale benaderingen zijn. Ook is vastgesteld dat er op pan-Europese niveau onvoldoende capaciteit is om vroegtijdig te kunnen waarschuwen tegen grote ICT-incidenten én dat er te weinig responscapaciteit is.

Wat zijn nu de acties:
1. Breng de paraatheid en preventie binnen alle Europese landen op een basisniveau om zo beter te kunnen samenwerken binnen Europa. Het ENISA kan hierbij belangrijk werk verrichten.
2. Voorzie in EU brede systemen voor detectie om vroegtijdige waarschuwingen mogelijk te kunnen maken.
3. Zorg voor responsplannen en oefeningen om bestrijding van een incident en het herstel daarvan mogelijk te maken. Iedere EU lidstaat die nog geen nationale CERT heeft zal er één moeten oprichten zodat alle EU CERT's meer met elkaar kunnen en moeten gaan samenwerken.
4. Leg criteria vast op basis waarvan de Europese vitale infrastructuren geïdentificeerd kunnen worden. Daarmee wordt alvast invulling gegeven aan het ICT deel van de EPCIP richtlijn.

In juni is er over deze mededeling in Tallinn een conferentie georganiseerd en tot genoegen van de Commissie bleek er ruime ondersteuning bij de lidstaten voor de mededeling.
Het vervolg
De Commissie gaat samen met de lidstaten in de komende twee tot drie jaar deze actielijnen uitvoeren. Zo zal er onderzocht worden in hoeverre het haalbaar is om een oefening te houden waar zo veel mogelijk EU landen bij betrokken zijn, zal de ontwikkeling en uitbouw van CERT's in Europa worden gestimuleerd, en zal worden gebouwd aan gemeenschappelijke respons-capaciteit binnen Europa.
De Commissie heeft ook duidelijk gesteld dat in het verdere CIIP proces de private sector intensief betrokken moet zijn, zo mogelijk via publiekprivate samenwerking op EU niveau. Een aspect waar Nederland (en ook de Scandinavische landen) goede ervaringen mee heeft en veel waarde aan hecht. Dat het de Commissie ernst is moge duidelijk worden uit het feit dat men de mededeling al tegen het eind van 2009 wil omzetten in een Raadsresolutie, waarmee het ook de politieke zegen van de lidstaten krijgt.

[2] Communication on Critical Information Infrastructure Protection, COM(2009) 149

Pauline Veldhuis-Beem,
parttime senior coördinerend beleidsmedewerker BZK,
Washington DC area/ VS (pauline.veldhuis@minbzk.nl)

Cybersecurity in de VS: een president en een tsaar

Tijdens zijn verkiezingscampagne beloofde president Obama om de cybersecurity, de veiligheid van computersystemen en het veilig gebruik van internet, tot een topprioriteit te maken. Zijn plannen presenteerde hij eind mei 2009. Hoe innovatief en verstrekkend zijn Obama's plannen en wat betekenen ze voor de private sector, voor burgers en niet te vergeten voor de overheid zelf?

Computersystemen en internet zijn onmisbaar in het dagelijkse leven en vormen feitelijk de ruggegraat – en daarmee een vitaal belang – van de maatschappij en de economie. Tegelijkertijd zijn ze een dagelijks doelwit van criminele activiteiten, de cybercrime. Zo maakte de *The Wall Street Journal* in april jl. melding van een inbraak in de computersystemen van het ministerie van Defensie. Hierbij zou uiterst gevoelige informatie over de *Joint Strike Fighter*, een nieuw gevechtsvliegtuig, zijn gestolen. In mei jl. bevestigde Obama in algemene termen de toenemende dreiging en gevolgen van cybercrime voor de overheid in het algemeen en voor defensie in het bijzonder. Daarnaast maakte hij melding van de gevolgen van cybercrime voor de private sector en voor burgers. Cybercrime, zo concludeerde Obama, vormt één van de grootste bedreigingen voor de economie en de nationale veiligheid van de VS.
Een onderzoek[1], in opdracht van Obama uitgevoerd, bevestigt dat de VS op dit moment, en zonder ingrijpende maatregelen ook in de toekomst, niet voldoende is toegerust om de toenemende dreiging van cybercrime het hoofd te kunnen bieden. Obama heeft op basis van dit onderzoek aangekondigd dat er ingrijpende maatregelen nodig zijn om de cybersecurity te verbeteren. Een constatering die met brede instemming is ontvangen. De maatregelen die Obama in een persconferentie op 29 mei 2009 heeft afgekondigd strekken zich uit tot de overheid, de private sector, de wetenschap, het onderwijs, de burgers en de internationale bondgenoten.

Samengevat komen de beleidsvoornemens voor cybersecurity neer op het ontwikkelen van een nieuwe strategische visie voor de nationale overheid. Het op deze visie gebaseerde beleid moet concreet en meetbaar zijn. Daarnaast moeten afspraken worden gemaakt tussen de nationale overheid, de staten, de lokale overheden, private partners en internationale bondgenoten.
Deze afspraken moeten een gecoördineerde reactie van de partners waarborgen zodra de veiligheid van computersystemen en internet in het geding is.
Wetenschappelijk onderzoek en het opleiden van voldoende specialisten moet ervoor zorgen dat nu en in de toekomst voldoende kennis en ervaring beschikbaar is. Ook de burger wordt niet vergeten.
Voorlichtingscampagnes zullen het publieke bewustzijn ten aanzien van cybersecurity moeten vergroten.

Innovatief beleid?

Het wordt als een positief signaal beschouwd dat Obama het onderwerp tot een persoonlijke prioriteit rekent. Maar dat betekent niet dat Obama de eerste president is die cybersecurity tot een nationale beleidsprioriteit maakt. Dat was destijds president Clinton. En het was de toenmalige president Bush die in 2003 de eerste nationale strategie op dit gebied, de *National Strategy to Secure Cyberspace*, lanceerde.
Ook voorlichtingscampagnes zijn al enkele jaren een vast onderdeel van het beleid. Tot zover lijkt er nog geen sprake van een nieuw en innovatief beleid.
Nieuw is in elk geval wel de (voorgenomen) aanstelling van een *cyberczar*, een "tsaar" die de cybersecurity moet gaan coördineren. Deze coördinator zal persoonlijk door Obama worden geselecteerd en zal een rechtstreekse toegang tot de president hebben. De taak van deze functionaris zal bestaan uit het regisseren en integreren van het overheidsbeleid op het gebied van de cybersecurity.

De reikwijdte van het nieuwe beleid

Obama heeft nadrukkelijk gesteld dat zijn beleid geen betrekking zal hebben op het monitoren van de private sector en het internet. Een opmerking die niet zomaar uit de lucht komt vallen. Privacybescherming is een belangrijk en gevoelig punt in dit dossier. Zeker nadat in het recente verleden werd vastgesteld dat onder de regering van president Bush regelmatig en zonder enige rechtsgrond het internetverkeer van particulieren en bedrijven werd gecontroleerd. Ook heeft Obama benadrukt dat hij geen verplichte normen aan de private sector zal opleggen.

[1] Het rapport is 29 mei 2009 gepubliceerd onder de naam: "Cyberspace Policy Review" (zie www.whitehouse.gov)

De uitdagingen

De eerste uitdaging is de benoeming van de coördinator. Er zijn maanden verstreken na de persconferentie in mei jl., maar een functionaris is nog steeds niet benoemd. Zwaargewichten voor de functie zijn absoluut voor handen, maar deze lijken geen van allen trek te hebben in de functie. En dat is om een aantal redenen verklaarbaar. Zo krijgt de coördinator een haast onmogelijke positie door veel verantwoordelijkheden te krijgen maar geen "doorzettingsmacht" om de opdracht uit te voeren. Zo zijn de taken en verantwoordelijkheden op dit beleidsdossier over verschillende ministeries en agentschappen versnipperd en deels overlappend. Dat dit problemen geeft blijkt bijvoorbeeld uit de openlijke machtsstrijd tussen het ministerie voor Binnenlandse Veiligheid (*Departement of Homeland Security*) en het ministerie van Defensie (*Department of Defense*). Defensie lijkt, met een sterke positie van de militaire veiligheidsdienst op het gebied van cybersecurity en een gigantisch budget, steviger in het zadel te zitten dan het ministerie van Binnenlandse Veiligheid. Een andere uitdaging is het gegeven dat Obama geen verplichte regels voor de private sector wil opstellen. Dat betekent dat een effectieve samenwerking op het gebied van cybersecurity afhankelijk is van de mate van bereidwilligheid van de private sector. Dat kan een effectief beleid belemmeren, temeer daar de informatie- en communicatienetwerken voor het merendeel in eigendom zijn van dezelfde private sector. Bovendien is het lastig om een strikte scheiding aan te brengen tussen netwerken van de overheid en de private sector. Dan is er ook nog de noodzaak tot voldoende technologische kennis en onderzoek. Het houden van een technologische voorsprong vraagt om hoog opgeleide deskundigen die bereid zijn om voor de publieke zaak te werken. Het zal de nodige investeringen vergen om de overheid voor dit type specialisten aantrekkelijk te maken. Het gaat niet alleen om geld, maar ook om het opkrikken van het negatieve imago van de overheid op dit vakgebied.

Een wetsontwerp

Begin april 2009 heeft senator John D. Rockefeller via een wetsvoorstel, de *Cybersecurity Act 2009*, duidelijk gemaakt dat hij een voorstander is van een strak geregisseerd beleid dat gebaseerd is op wettelijke normen voor de federale overheid en haar partners. De lijn van het wetsontwerp staat haaks op de beleidsplannen van Obama. Of het wetsvoorstel het gaat halen is zeer de vraag. Het is in elk geval niet enthousiast ontvangen door de private sector en organisaties voor privacybescherming.

Ten slotte

De toekomst zal moeten uitwijzen of het beleid voldoende effectief is om de cybersecurity ook in de 21ste eeuw te kunnen waarborgen. Dat er na maanden nog steeds geen coördinator is benoemd lijkt in elk geval geen veelbelovende start.

Gezamenlijke bijeenkomst **redactieraad** en **redactiecommissie**

Op 1 juli van dit jaar vond een eerste gezamenlijke bijeenkomst plaats van de redactieraad en de redactiecommissie van het Magazine. De leden van de redactieraad spelen op verschillende terreinen een belangrijke rol in de ontwikkeling van kennis en beleid op het gebied van nationale veiligheid en crisisbeheersing.

In de praktijk hebben de leden incidenteel contact met elkaar, maar de gezamenlijke participatie aan de redactieraad biedt een basis voor een verdere uitbreiding en verdieping van het kennisnetwerk op dit terrein. Tijdens de bijeenkomst in Sociëteit De Witte te Den Haag hield Ira Helsloot een exposé over actuele ontwikkelingen op het terrein van zelfredzaamheid bij crises, gevolgd door een geanimeerde inhoudelijke discussie. Hierna volgen kort en puntig de centrale stellingnamen van leden van de redactieraad rondom dit thema.

Stellingnames leden redactieraad over **zelfredzaamheid**

Hoe red ik mij uit de nesten

Ben Ale

Zelfredzaamheid is een recente tak aan de boom van rampenbestrijding en crisisbeheersing. We moeten allemaal een beetje of veel voor onszelf kunnen zorgen, al was het alleen maar omdat in tijden van grote crises de hulp even op zich zal laten wachten, of helemaal niet komt opdagen. Of je daartoe mogelijkheden hebt hangt er erg vanaf in welke conditie je bent, waar je woont en hoeveel geld je te besteden hebt.
Woon je in een flat in de stad dan zijn de mogelijkheden beperkt, vooral omdat je geen goede bron van energie kunt beginnen. Niettemin zou je kunnen overwegen een stel “powerpacks” opgeladen achter de hand te houden om de koelkast gaande te houden en wat licht. Een butagas brandertje is een goede oplossing om op te koken. Met wat voorraden in de vriezer kun je het dan al een tijd uitzingen. Als je water in voorraad neemt, denk er dan aan dat van tijd tot tijd te verversen. Als water erg oud is kun je het beter even koken.
Als je een huis hebt of toegang tot een dak heb je veel meer mogelijkheden. Met een regenton heb je niet alleen water voor de planten, maar ook water om te wassen en om het toilet door te spoelen. Om te drinken is regenwater iets minder geschikt, maar gekookt gaat het zelfs in Nederland nog wel.
De aanschaf van zonnecellen is dan niet alleen goed voor het milieu en de verlaging van je energierekening. Een setje zonnecellen levert genoeg energie voor de koelkast, de pomp en de thermostaat van de cv en voor licht en de computer, waarmee je toegang hebt tot internet en TV kunt kijken. Je kunt er bovendien batterijen mee opladen. Als je een open haard hebt of een houtkachel zorg dan voor een voorraad hout. Dan kun je daarmee ook koken. Led licht gebruikt veel minder energie dan spaarlampen. Als je ‘s nachts ook elektriciteit wil hebben dan ontkom je niet aan accu’s. Dan heb je of een omvormer nodig of een afzonderlijke 12V installatie. Dat laatste is een stuk energiezuiniger. Een eigen aggregaat in de schuur is goed genoeg voor gebruik van een heel gezin. Wel zorgen voor een brandstofvoorraad en die veilig opslaan.

De illusie van de zelfredzame burger

Arjen Boin

De zelfredzame burger wacht niet lijdzaam op de overheid die onmiddellijk bijstand komt verlenen in geval van nood. Integendeel, na de eigen familie in veiligheid te hebben gebracht, gaat deze burger aan de slag om anderen te redden. De burger die zichzelf redt: het Ei van Columbus.

Maar bestaat deze modelburger eigenlijk wel? De zelfredzame burger is een ontdekking van Amerikaanse rampenonderzoekers. Zij beschrijven hoe burgers de handen ineen slaan en zo de eerste dagen na een ramp overleven. Veel van de bestudeerde rampen zijn echter oude rampen. De Amerikaanse overheid bemoeide zich toen nog niet actief met crisis- en rampenmanagement. Zelfredzaamheid was simpelweg de enige optie. Dezelfde rampenliteratuur beschrijft ook rampen waar van zelfredzaamheid geen sprake is. De zelfredzame burger is dan ook geen wetmatigheid. De ramp in New Orleans vormt hier een nuttige reality check: de (zeer arme) bevolking van de ondergelopen stad kon zich niet redden zonder hulp van buiten.

De vraag is wat we in Nederland mogen verwachten. De Zeeuwse waterramp en de oorlogswinter stelden Nederlanders voor het laatst echt op de proef. Dat de huidige generatie Nederlanders zichzelf kan redden na een grootschalige ramp lijkt dan ook een optimistische veronderstelling. Zolang niet duidelijk is wat beleidsmakers kunnen doen om burgers zelfredzaam te maken, doen zij er goed aan het zelfredzaamheid concept te negeren. Beleidsmakers kunnen zich beter afvragen hoe zelfredzaam hulpdiensten en lokale instituties zijn. De zelfredzame overheid: daar is tijdens een ramp nog steeds de meeste behoefte aan. >>>

Self-reliance in Nieuw Zeeland

Ernst Brainich, werkzaam als manager emergency management in Nieuw Zeeland

Als een aardbeving zoals die eind september in de Stille Oceaan plaatsvond, Wellington zou treffen, is de stad naar verwachting dagen van de buitenwereld afgesloten. Dat betekent dat al die tijd mensen, slachtoffers, op zichzelf zijn aangewezen. In het gebouw waar ik werk staan op elke verdieping containers met nooddrinkwater; er staan kasten met noodrantsoen; mensen hebben in hun bureaus sportschoenen en extra kleding. De verwachting is dat – bij een aardbeving overdag – mensen in de stad moeten blijven bivakkeren; zodra dat kan, zullen zij naar hun huizen buiten de stad gaan lopen.
Het eerste principe van de crisisbeheersingsstrategie van Nieuw Zeeland heeft geen enkele betrekking op de respons van overheden: het betreft de eigen verantwoordelijkheid van individuen, bedrijven en leefgemeenschappen: *You need to be able to look after yourself in an emergency*. Nieuw Zeeland ligt op een breukvlak. Geregeld voel je hier trillingen. En in het noorden is er de kans op vulkanische uitbarstingen. Dat maakt dat men zich hier zeer bewust is van mogelijke crises. Zelfredzaamheid is daarbij een geaccepteerd gegeven. En dat is niets nieuws in een land waar – net als in Australië – nogal wat mensen *in the middle of nowhere* wonen. Ik denk ook dat het past bij een pionierscultuur.
Het lijkt me niet reëel om een dergelijke houding van mensen in Nederland te verwachten. De kans op crises moet heel tastbaar zijn, wil zo'n niveau van crisisbewustzijn en preparatie normaal zijn. Dat betekent niet dat Nederlanders niet zelfredzaam zijn of zouden kunnen zijn, maar de individuele voorbereiding is veel minder of non-existent. En afhankelijk van het type crisis kan dat meer werk voor overheden betekenen. Burgers zijn niet afwachtend en hulpeloos, maar als er in steden gebrek is aan drinkwater en voedsel, zal er toch iets moeten gebeuren. We zeggen dat crisisbeheersing moet liggen in het verlengde van het normale beleid.
Iets vergelijkbaars geldt ook voor individuele preparatie: dat werkt alleen maar als het past in de bestaande cultuur. Initiatieven van overheidswege veranderen daar niets aan.

Realistisch blijven

Ira Helsloot

Zelfredzaamheid is goed, zelfredzaamheid is beter, lang leve de zelfredzaamheid! Het is daarmee goed dat de waardering voor zelfredzaamheid bij de overheid toeneemt, maar laten we op twee punten realistisch blijven.
Het eerste punt is dat burgers en bedrijven zelfredzaam zijn tijdens crises, maar dat betekent niet dat zij zich voorbereiden op crisis. Alle beschikbaar onderzoek laat zien dat mensen zich niet voorbereiden op incidenten waarvan zij de kans van voorkomen (al dan niet terecht) laag in schatten. Zolang de overheid dus bijvoorbeeld communiceert dat wij veilige dijken hebben (en dat hebben we) dan zal niemand zich werkelijk gaan voorbereiden op een grootschalige overstroming, Dat geldt voor zowel overheden als burgers en bedrijven.
Het tweede punt is dat, om Job Cohen te citeren, je natuurlijk de plicht hebt als overheid om de zelfredzaamheid van burgers zo goed mogelijk te faciliteren, maar dat je als overheid toch na elke crisis zult worden aangesproken op het falen van de preventie. Meer precies geldt volgens mij dat als je als overheid niet vooraf helder onveiligheid durft te communiceren en de beperkingen van de hulpverlening durft toe te geven, dat je dan achteraf niet kunt hopen op een milde burger omdat je 'toevallig' de zelfredzaamheid van die burger goed hebt gefaciliteerd.

Vertrouwen in veerkracht samenleving

Menno van Duin

Er is een discussie of en in hoeverre je zelfredzaamheid van burgers kan stimuleren en bevorderen. Ik geloof heilig in bepaalde specifieke vormen van voorlichting. Veel mensen zijn geïnteresseerd om te weten wat ze moeten doen bij brand of bij het te water komen met je auto. Dergelijke voorlichting is – uiteraard met de moderne media; dus veel filmpjes e.d. – zinvol. Ik kan me heel goed voorstellen daar landelijk filmpjes voor te ontwikkelen en die via verschillende sites (uiteraard crisis.nl/denkvooruit.nl) maar ook actiever te verspreiden. In de discotheek zou 'Waar is hier de nooduitgang' gewoon standaard 1 minuut moeten worden gedraaid en dat worden begeleid met lichten die naar deze uitgangen leiden. Daarbij moet steeds volledig worden aangesloten op de wensen van de klanten/burgers. Korte, beeldende informatie voor specifieke risico's. Ook voor specifieke groepen (bijvoorbeeld gehandicapten) zou – opnieuw aansluitend bij hun wensen! – informatie en beeldmateriaal moeten worden gemaakt.
Ik heb geen behoefte aan allerlei vormen van algemene informatie over wat mensen in rampen en crises zouden moeten doen. Dat ze dan elkaar zouden moeten helpen; routes vooraf uitstippelen; voorraden in huis halen; spaarzaam zijn met telefoongebruik e.d. In dergelijke informatie heb ik weinig vertrouwen. Wij kunnen en moeten – op grond van veel internationaal onderzoek – ervan uitgaan dat in dergelijke situaties betrokkenen vrij goed in staat zijn zelfredzaam te zijn. De meeste hulp in grote crises komt van familie en omstanders; gewonden bereiken veelal met hulp van particulieren ziekenhuizen e.d. In echte noodsituaties – waar professionele hulp niet voldoende is – heb ik vertrouwen in de veerkracht van de samenleving.

Zelfredzaamheid als trend

Erwin Muller

Zelfredzaamheid is het nieuwe modewoord in crisisbeheersing en rampenbestrijding. Burgers en bedrijven moeten meer zelfredzaam zijn in de veiligheidszorg in het algemeen en tijdens crisis en rampen in het bijzonder. Wat zelfredzaamheid betekent is echter niet helemaal duidelijk. Soms gaat het om het daadwerkelijk verbeteren van de competenties van burgers (en bedrijven) om zich te kunnen redden in onveilige situaties. Soms lijkt het erop dat het gaat om verantwoordelijkheden van de overheid af te schuiven op burgers. Soms lijkt het ook op een ordinaire bezuiningsmaatregel. In andere gevallen is het oprecht verbeteren van de informatievoorzieningen aan de burgers. De mode verandert net zo snel als de definitie van zelfredzaamheid.
Iedereen is het er over eens dat de overheid niet alleen in staat is om veiligheid te garanderen en tijdens crisis en rampen burgers te redden. Dit inzicht is al oud en weinig modern. Veel veiligheidsorganisaties zoals de politie en de brandweer zijn oorspronkelijk ontstaan uit initiatieven van burgers om de sociale en fysieke veiligheid te realiseren. Zelfredzaamheid was vroeger eerder regel dan uitzondering. Sinds wij de belangrijke taken op het gebeid van veiligheidszorg, crisisbeheersing en rampenbestrijding aan complexe instituties zoals de politie, brandweer, ambulancezorg, defensie en anderen hebben overgedragen is de zelfredzaamheid van burgers afgenomen. Nu beginnen deze instituties te beseffen dat zij niet in staat zijn de omvangrijke verwachtingen van burgers ten aanzien van veiligheid te realiseren.
De burgers (en bedrijven) zijn weer zelf nodig. Gelukkig herhaalt de geschiedenis zich steeds zodat enige voorspelbaarheid mogelijk is.

DENK VOORUIT

>>>

Divergentie in zelfredzaamheid en overheidsmanagement

Astrid Scholtens

Het omgaan met het fenomeen (zelf)redzaamheid is in de wereld van rampenbestrijding en crisisbeheersing een lastige, omdat deze wereld zich kenmerkt door coördinatie- en sturingsmechanismen en het volgen van (beoefende) procedures. Internationaal onderzoek laat zien dat zelfredzaamheid spontaan gebeurt en dat (zelf)zame burgers zich daarbij niet laten sturen. De zelfredzame burger houdt 'slechts' rekening met zijn eigen altruïsme tijdens crisisomstandigheden en de zorg voor zijn familie en vrienden.
Het 'onstuurbare optreden' van de zelfredzame burger sluit daarmee niet aan bij het huidige concept van het overheidscrisismanagement. Of wellicht beter geformuleerd: het huidige concept van het overheids-crisismanagement sluit niet aan bij het fenomeen zelfredzaamheid. En terwijl 'het veld' nadenkt over de vraag wat er precies moet gebeuren om beide werelden beter op elkaar te laten aansluiten, vraag ik mij af of een dergelijke divergentie een onoverkomelijk probleem is. Voor onderzoeksdoeleinden is het misschien nuttig om eens uit te gaan van het standpunt dat het overheids-optreden bij crises onvermijdbaar parallel loopt aan en niet af te stemmen is met het handelen van de zelfredzame burger. Laten we eens goed nadenken waar dit standpunt ons brengt.

Er is niets nieuws onder de zon, verzuchtte de Prediker

Erwin Seydel

Wie googled op het begrip ' zelfredzaamheid' scoort 191000 hits. Autisten moeten zelfredzaam worden, WMO-ambetnaren vragen zich af waar je hulpeloze mensen vindt, zodat zij zelfredzaam worden. De doorsnee burger ontbeert digitale zelfredzaamheid, kopt een ochtendkrant. Bouman, hoofdredacteur van Archis, vindt dat "de kunstenaar zich meer moet bezighouden met de kwetsbare groepen in de samenleving. Hun zelfredzaamheid zou vergroot kunnen worden door 'interactieve' kunstprojecten." NOS-onderzoeksjournalist Robert Bas meldt dat de overheid niet steeds moet verkondigen dat je alles onder controle hebt!"
COT-directeur Erwin Muller geeft toe dat het stimuleren van zelfredzaamheid in de risicocommunicatie – na de opheffing van de Bescherming Bevolking (BB) – terug bij af is. "We zijn dat terrein angstig aan het verkennen, maar daar zit wat mij betreft de echte uitdaging." Ik sluit me graag aan bij deze constatering. Maar we moeten er wel voor oppassen dat al die goed bedoelde zelfredzaam-heidadviezen door de burger niet wordt geïnterpreteerd als 'zoek het zelf maar uit'.
Er is niets nieuws onder de zon, verzuchtte de Prediker. Daar heeft hij wel een beetje gelijk in. Al vijfhonderd jaar voor Christus noemde de trotse oude Grieken zelfredzaamheid *autarkeia*. De eerlijkheid gebiedt te zeggen, dat zij daarin in het onvruchtbare Griekenland slechts zelden volledig in slaagden. Vaak moest een gemeenschap bij voorbeeld een deel van haar voedsel met hulp van de overheid elders halen.
Gelukkig heeft het grootste deel van onze bevolking nog geen flauw benul waarin ze zelfredzaam moet zijn, laat recent onderzoek zien, maar ze reageert als het nodig is puur intuïtief. Toch een uitdaging?

Overheid kan ook leren van burgers

Peter Werkhoven

In het laatste decennium is het denken over crisisbeheersing gekanteld van een volledig verantwoordelijke overheid, naar een zorgzame en informerende overheid met eigen verantwoordelijkheid van burgers. Adequate crisisbeheersing zou gebaat zijn bij een verdere kanteling waarbij burgers niet alleen van de overheid leren, maar de overheid ook van de burgers leert.
Burgers zijn bij een crisis behoorlijk zelfredzaam (60%-90% redt zichzelf of wordt door andere burgers gered), in staat tot rationeel denken, en het is een mythe dat ze snel in paniek raken. Op basis van de huidige overheidscampagnes zal een rationeel burger zich echter niet specifiek voorbereiden. Deze campagnes geven burgers namelijk informatie om adequaat te laten beslissen bij een crisis, maar zeggen tegelijkertijd dat de kans erg klein is dat het nodig is.
Risicoperceptie en gedrag van burgers kan veel effectiever beïnvloed worden via 'community interventions'.
Meningen en gedragingen van sleutelfiguren in een community bepalen sterk de risicoperceptie van de andere leden en daarmee tevens hoe serieus de overheid wordt genomen. Het is verder bekend dat de belangrijkste informatiebron voor burgers de burger zelf is. In diezelfde communities is namelijk een schat van locale ervaring en kennis aanwezig over locale risico's, beschikbaarheid van middelen en hulpbehoevendheid. In een interactie tussen overheid en communities kan deze kennis worden aangeboord en kan veel worden geleerd op zowel operationeel als beleidsniveau (crowd sourcing).
Dus om de zelfredzaamheid van burgers te beïnvloeden én het leren van burgers mogelijk te maken zijn interacties in en met communities nodig. Deze combinatie pleit voor een gerichte inzet van social media zoals serious gaming, zowel gericht op bewustwording van burgers als op crowd sourcing.

Zelfredzaam ben ik in Frankrijk

Rob de Wijk

Zelfredzaamheid betekent 'jezelf kunnen redden'. Logisch eigenlijk. Maar wat zijn de beleidsimplicaties voor rampenbestrijders en crisisbeheersers die dit begrip omarmen als het nieuwe paradigma? Is het 'wij kunnen weinig, dus red je zelf maar'? Ik hoop van niet. Als burger wil ik dat mijn zelfredzaamheid wordt gefaciliteerd. Kijk naar vliegen. De noodprocedures die voor het opstijgen worden uitgelegd, moeten de zelfredzaamheid vergroten. Ik heb vaak nagedacht over zelfredzaamheid in mijn eigen omgeving, zeker ten tijde van Oefening Waterproef. Wij wonen in het putje van Nederland, dus tijdens een watersnood houden wij het niet droog. Maar wat kan ik doen? Alle wegen staan vol met vluchtende medeburgers. Ik heb geen idee of alle rijbanen van de A12 voor het uitgaande verkeer kunnen worden gebruikt. En ik weet niet waar ik mij moet melden. Wel heb ik bedacht dat ik de auto laat staan en mij op de motor door de file wring op weg naar het hooggelegen huis van mijn moeder. Maar of ik dat haal is twijfelachtig als ik bij het benzinestation niet kan pinnen omdat de stroom eruit ligt. Als het hier echt fout gaat hoop ik dat ik mijn huisje in Frankrijk kan bereiken. Het dorp kent nog onderlinge solidariteit, zelfs naar buitenlanders. Er is altijd wel iets te eten. We stoken en koken op hout en er is een bron. En bij kaarslicht valt best te lezen. Iedere keer als ik daar ben voel ik hoe kwetsbaar we in de drukbevolkte Randstad zijn en hoe afhankelijk van anderen bij een ramp. Zelfredzaam ben ik in Frankrijk.

Floor Keijsers,
projectleider Denk Vooruit-campagne

Denk Vooruit in 2009: is uw noodpakket al compleet ?

Uitgangspunt 1: in Nederland kunnen noodsituaties ontstaan en die kunnen we niet altijd voorkomen. Uitgangspunt 2: als er een noodsituatie is, kunnen hulpdiensten niet iedereen tegelijkertijd helpen. U moet zichzelf dus in veiligheid kunnen brengen. Uitgangspunt 3: U bent zelfredzaam tijdens een noodsituatie. Uitgangspunt 4: zelfredzaam zijn betekent niet automatisch dat u zich ook voorbereidt op een noodsituatie, blijkt uit onderzoek. En dat is jammer, want uit ander onderzoek blijkt dat zelfredzame mensen door een gebrek aan voorbereiding en informatie in een noodsituatie soms (achteraf bezien) verkeerde beslissingen nemen. Als u voorbereid bent op een noodsituatie, kunt u zichzelf en anderen beter helpen. En om dit laatste voor het voetlicht te brengen, is er de Denk Vooruit-campagne. De Denk Vooruit-campagne van 2009 loopt van 29 oktober tot en met 6 december.

De Denk Vooruit-campagne van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) moet Nederlanders bewust maken van het feit dat ook in ons land noodsituaties kunnen ontstaan. En dat het handig is je daarop voor te bereiden. Want in sommige situaties wordt niet iedereen tegelijkertijd geholpen door de hulpdiensten. Zij helpen eerst de mensen die hun hulp het hardst nodig hebben. En dat betekent dat veel mensen enige tijd op zichzelf zijn aangewezen. Op zulke momenten is een noodpakket handig, want in een noodpakket zitten spullen (onder andere een opwindbare radio, kaarsen en warmhouddekens) die helpen bij bijvoorbeeld stroomuitval en overstromingen. Met het noodpakket proberen we het voorbereiden op noodsituaties concreet en tastbaar te maken.

Veel spullen heeft u al in huis

Natuurlijk hoeft u geen kant-en-klaar noodpakket te kopen; veel spullen heeft u al in huis. Het enige wat u moet doen, is de spullen te verzamelen (het liefst in een waterdichte verpakking) en op een handige plek te bewaren. En als u toch liever kiest voor een kant-en-klaar pakket, dan kan dat ook. Inmiddels zijn er verschillende aanbieders van noodpakketten op de markt. Een noodpakket dat u in de winkel koopt, is niet helemaal aan uw persoonlijke situatie aangepast. Soms is het nodig om het aan te vullen. Bijvoorbeeld met medicijnen of kindervoeding. Zorg ook dat u voldoende eten en drinken in huis hebt.
Kijk op http://denkvooruit.nl/noodpakket voor meer informatie over de inhoud van een noodpakket.

Handig bij groot en klein ongemak

Een noodpakket is niet alleen handig tijdens grote noodsituaties. Ook bij huis-, tuin- en keukenongevallen is een noodpakket bruikbaar. Zo komt de EHBO-set goed van pas bij bijvoorbeeld schaafwondjes of bloedingen. Om dit te benadrukken, heeft BZK samen met Het Oranje Kruis de folder '8 *Eerste* Eerste Hulp Tips' uitgebracht.
De folder is verkrijgbaar bij bibliotheken, kringapotheken, consultatiebureaus, verloskundigenpraktijken en wachtkamers van ziekenhuizen.

De Denk Vooruit-campagne in 2009: wat merkt u ervan?

In 2009 wordt van 26 oktober tot en met 6 december landelijk campagne gevoerd voor Denk Vooruit. Tijdens de campagneperiode wordt u via tv- en radiospots geïnformeerd over het voorbereiden op noodsituaties. Iedere eerste maandag van de maand (als de sirenes worden getest) hoort u één van onze spots op de radio. In deze spot wordt u de vraag gesteld of u weet wat u moet doen als de sirene gaat. In de tweede spot staat (de inhoud van) het noodpakket centraal.
Behalve de tv- en radiospots maken we ook gebruik van internetbanners en de website www.denkvooruit.nl. Op de website is achtergrondinformatie te vinden over het voorbereiden op noodsituaties.
Naast de landelijke campagne heeft een groot aantal gemeenten en regio's lokale en regionale campagnes opgezet. De meeste van deze campagnes haken aan bij de landelijke Denk Vooruit-campagne, maar vertalen de algemene boodschap ('bereid je voor') naar een specifieke boodschap voor de gemeente of regio. En dat is ook precies de bedoeling. Want waar de landelijke campagne vooral bedoeld is om via massamediale kanalen bekendheid te genereren voor voorbereiden, kunnen gemeenten en regio's inspelen op specifieke gebeurtenissen of risico's in hun omgeving. En daardoor wordt de boodschap relevanter en wellicht ook interessanter voor de inwoners.

Floor Keijsers,
projectleider campagne Denk Vooruit
Anja van den Bosch-Overduin,
communicatiemedewerker specifieke doelgroepen voor de campagne Denk Vooruit

Succesvolle pilot Denk Vooruit-campagne in virtueel jongerenhotel

Hoe bereik je jongeren in de leeftijd van 12 tot 18 jaar, die steeds minder televisie kijken en radio luisteren en steeds meer online doen? Juist, door zelf óók online te gaan. Dat was wat het ministerie van Binnenlandse Zaken onlangs deed met de Denk Vooruit-campagne. Van 25 mei tot en met 21 juni 2009 konden de jonge bezoekers van Habbo (de grootste virtuele jongerencommunity van Nederland) deelnemen aan allerlei leuke en leerzame activiteiten rondom de voorbereiding op noodsituaties. In dit artikel geven we een overzicht van de belangrijkste uitkomsten.

27.763 enthousiaste deelnemers

In het virtuele Habbo-hotel werd een maand lang een rampenoefening georganiseerd. Deze rampenoefening bestond uit meerdere activiteiten, waaronder een evacuatie-quest over 'wat te doen als de sirene gaat' en het ontwerpen van een eigen veiligheidsfolder. Ook konden de jongeren meedoen aan een evacuatie voor een denkbeeldige overstroming. Doelstelling van deze activiteiten: jongeren bewust maken van het feit dat ook zij kunnen worden getroffen door een noodsituatie en dat het verstandig is je daarop voor te bereiden. In totaal hebben 27.763 jongeren actief meegedaan aan de activiteiten; tachtigduizend jongeren bezochten de Denk Vooruit-bibliotheek op habbo.nl. In vergelijking met andere campagnes binnen Habbo is dit erg veel.

Uit een evaluatie van de Habbo-pilot, opgesteld op basis van de antwoorden op een poll (online-enquête) en een case study van de bezoekersaantallen, blijkt dat de pilot erg succesvol is geweest. Onderstaand de belangrijkste resultaten op een rij:

Belangrijkste poll-resultaten

- Jongeren die hebben deelgenomen aan de Denk Vooruit-pilot, beoordelen de pilot met een acht. Dit is hoger dan de beoordelingen van de meeste andere Habbo-campagnes.
- In de 0-meting gaf 50% van de jongeren aan de Denk Vooruit-campagne te kennen; in de eindmeting was dat 75%.
- Jongeren zijn het meest bang voor een terroristische aanslag (0-meting 34%, eindmeting 33%).
- Het minst bang zijn jongeren voor een kernongeval (0-meting 0.49%, eindmeting 0.62%).
- Ongeveer 70% van de jongeren vindt het belangrijk dat in Habbo aandacht wordt besteed aan het voorbereiden op noodsituaties.
- 60,77% van de jongeren geeft aan veel of redelijk veel geleerd te hebben van de pilot.

Belangrijkste resultaten uit de case study

- Tijdens de pilot hebben 27.763 jongeren deelgenomen aan de Denk Vooruit-activiteiten (quiz, evacuatie-quest en pixel art).
- 80.000 jongeren bezochten de Denk Vooruit-bibliotheek. 15.7% van deze jongeren klikte door naar de Denk Vooruit-website. Dit is een erg hoog percentage; normaal gesproken ligt het click through-percentage op ongeveer 4%.
- 6.963 jongeren hebben deelgenomen aan de evacuatie-quest.
- 106 jongeren hebben meegedaan aan de pixel art-competitie, waarbij ze een eigen rampenfolder moesten ontwerpen. 4.062 jongeren stemden op de inzendingen.

Verschillende media besteedden aandacht aan de Denk Vooruit-campagne in Habbo. Zo verschenen er berichten in diverse kranten, op radio en televisie (waaronder het Jeugdjournaal). Al met al kan de proef met het benaderen van jongeren via een online omgeving dus als geslaagd beschouwd worden. Jongeren blijken zeker geïnteresseerd in de manier waarop zij zich zouden kunnen voorbereiden op noodsituaties en denken hier graag actief over na. Aangetoond is dat ook een 'zwaar' onderwerp zich leent om via een online omgeving te bespreken. Op korte termijn wordt bekeken of deze pilot een (rijksbreed) vervolg gaat krijgen.

Meer informatie

www.habbo.nl
www.denkvooruit.nl

Kwart bevolking treft voorbereidingen voor ramp of noodsituatie

Een kwart van de bevolking heeft zich voorbereid op een ramp of een noodsituatie. Meestal door het in huis halen of hebben van praktische gebruiksvoorwerpen (waxinelichtjes, gereedschap, een zaklamp en een EHBO-doos) of met een noodvoorraad voeding en water. Een meerderheid (63 procent) vindt het belangrijk artikelen voor een noodsituatie te hebben, en heeft ook al veel van deze spullen voor algemeen gebruik in huis. Belangrijke dingen die in de meeste huishoudens nog ontbreken zijn warmhouddekens (37 procent), een radio met batterijen (36 procent) en lucifers in waterdichte verpakking (19 procent). Mannen beschikken vaker over deze spullen dan vrouwen.

Dit blijkt uit onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties door de onderzoeksbureaus ISIZ en Stadspeil in Amsterdam. Het onderzoek vond plaats rond de campagne 'Denk Vooruit', waarmee het ministerie mensen ervan bewust wil maken dat ook in ons land rampen en noodsituaties kunnen voorkomen en dat voorbereiding nuttig is.

De meeste mensen denken dat de kans om getroffen te worden door een ziektegolf het grootst is (27 procent vindt dit risico tamelijk of zeer groot), gevolgd door het vrijkomen van gevaarlijke stoffen (14 procent), een ernstig verkeersongeval (12 procent) en een grote brand (12 procent). De kans dat ze te maken krijgen met ordeverstoringen, een overstroming, extreem weer of een langdurige uitval van stroom, gas of water, schatten de meeste mensen laag in (6 à 8 procent). Slechts 2 à 3 procent van de mensen vindt de kans op een terroristische aanslag of kernramp tamelijk of zeer groot.

De ingeschatte kans staat los van waar mensen bang voor zijn. Het bangst (25 procent) zijn mensen om in een grote brand terecht te komen. Daarna komen de angst voor het vrijkomen van gevaarlijke stoffen, een aanslag en een kernramp (allemaal 10 procent). Voor een ziektegolf of griepepidemie is slechts 6 procent echt bang, terwijl zij de kans hierop wel het hoogste inschatten.

In geval van nood verwacht men van de overheid vooral snelle en adequate afhandeling van de situatie (64 procent) en goede voorlichting (21 procent). Telefonische bereikbaarheid van de overheid scoort slechts 4 procent.

Overige resultaten:

- Mannen zetten in een noodsituatie eerder radio of tv aan dan vrouwen.
- Meer dan de helft van de bevolking zegt in geval van nood als eerste familieleden in veiligheid te zullen brengen. Mannen (75 procent) zouden vaker de veiligheid van hun gezinsleden proberen te waarborgen dan vrouwen (58 procent). Vrouwen denken relatief vaak als eerste aan hun huisdieren.
- Mensen bellen in geval van nood als eerste hun partner, gevolgd door de kinderen en de ouders.
- Het overgrote deel van de bevolking denkt dat de kans op een noodsituatie het grootst is in grote steden (70 procent), gevolgd door 16 procent die denkt dat die kans aan de kust het grootst is. Toch hebben mensen geen voorkeur om in het geval van een noodsituatie in een stad, dorp of een plaats buiten de bebouwde kom te zijn. Men voelt zich dus niet uitgesproken veiliger in een stad of in een dorp.

Vooral langs een spoorlijn waar gevaarlijke stoffen vervoerd worden, in de buurt van een kerncentrale en op de snelweg verwacht men sneller in een noodsituatie terecht te komen.

(Bron: persbericht ministerie van BZK, 12 november 2009)

Het Carnegie Heldenfonds en (zelf)redzaamheid

Hans W. de Vries,
secretaris Stichting Carnegie Heldenfonds

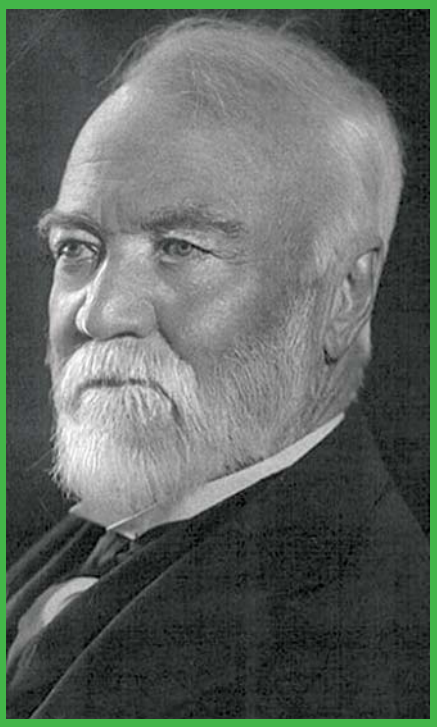
Het Carnegie Heldenfonds is relatief onbekend bij zowel het grote publiek als ook bij bestuurders en professionele hulpverleners. Dit is jammer, omdat juist dit fonds burgers kan stimuleren om bij ongevallen niet werkeloos aan de kant te blijven staan maar als het even kan hulp te bieden; (zelf)redzaam te zijn dus! Natuurlijk is het niet zo dat het vooruitzicht op een onderscheiding burgers in actie brengt. Wél kan bij voorbeeld publiciteit die de media doorgaans geven aan de uitreiking van een onderscheiding aan de helden, mensen aan het denken zetten. Een goed voorbeeld doet immers goed volgen.

Wat is het Carnegie Heldenfonds?
De Stichting Carnegie Heldenfonds werd door Andrew Carnegie (bekend van de Carnegie Hall in New York en het Vredespaleis in Den Haag) in 1911 met hulp van de Nederlandse regering opgericht. Carnegie stelde een flink bedrag beschikbaar. Daarvóór, in 1904, richtte hij al een dergelijk fonds op in de Verenigde Staten. Hij deed dit nadat zich een enorme explosie voordeed in een kolenmijn in de buurt van Pittsburgh, die aan 178 mensen het leven kostte. Bij de reddingspogingen kwamen twee mannen om het leven. Zij lieten een gezin met jonge kinderen achter. Carnegie vond dat de achtergebleven gezinnen (financiële) ondersteuning moesten krijgen.

Wat doet de stichting?
In lijn met de wensen van Carnegie kan de stichting een onderscheiding toekennen aan mensen die met gevaar voor eigen leven het leven van anderen hebben gered of gepoogd te redden. Ook is het mogelijk om deze helden of hun nabestaanden zo nodig van geldzorgen te bevrijden die het gevolg zijn van hun moedig gedrag. Sinds een paar jaar is het ook mogelijk om personen te onderscheiden die met gevaar voor zichzelf (geen levensgevaar) voor anderen in de bres zijn gesprongen. De stichting kent jaarlijks zo'n 40 tot 50 onderscheidingen toe. Ze worden meestal uitgereikt door de burgemeester die de voordracht heeft gedaan. Een voordracht kan echter door iedereen gedaan worden.

Bekendheid
Zoals gezegd is het fonds niet zo bekend, al bestaat het over een paar jaar al 100 jaar. Het bestuur, onder voorzitterschap van Jan Franssen, commissaris van de Koningin in Zuid-Holland, wil daar de komende tijd door gerichte acties verandering in brengen en daarmee het aantal voordrachten voor een onderscheiding laten groeien. Dat zou ook nog eens prima kunnen passen in de bevordering van Verantwoordelijk Burgerschap!

Voor meer informatie:
www.carnegiefonds.nl



Pauline Veldhuis-Beem,
parttime senior coördinerend beleidsmedewerker BZK,
Washington DC area/ VS (pauline.veldhuis@minbzk.nl)

Wie overleeft een ramp en waarom?

Zelfredzaamheid van burgers is een onderwerp dat zowel in Amerika als in Nederland hoog op de politieke agenda staat. Daarom in dit artikel aandacht voor een boek van de Amerikaanse journaliste Amanda Riply dat in 2008 is verschenen is onder de titel “The Unthinkable. Who survives when disaster strikes- and why”. Het boek gaat over zelfredzaamheid van burgers direct na een ramp, voordat hulpverlening ter plaatse is. Wat ervaren mensen op zo’n levensbedreigend moment, wat doen ze, wat doen ze niet en waarom? En wat kunnen burgers en beleidsmakers hiervan leren?

Riply beschrijft in haar boek drie fasen waarmee slachtoffers direct na een ramp worden geconfronteerd. Zij doet dit aan de hand van persoonlijke ervaringen van slachtoffers van verschillende rampen en incidenten. Met behulp van deskundigen en wetenschappelijk onderzoek legt ze vervolgens het “waarom” van het menselijk gedrag uit. Riply maakt geen onderscheid tussen rampen en gewone incidenten. Zij stelt dat ongeacht de aard of omvang van het incident het slachtoffers steeds met dezelfde fasen zal worden geconfronteerd.

Drie fasen na een ramp

In de eerste fase direct na een ramp is er sprake van ongeloof (“waarom moet mij dit nu overkomen”) of gewoonweg het volkomen negeren van de gebeurtenis (“hier wil ik niets mee te maken hebben”). De meeste slachtoffers zijn rustig of gedragen zich onverschillig ten opzichte van de gebeurtenis. Riply noemt deze eerste fase de ontkenningsfase.
De tweede fase is die van het overleg, het wikken het wegen van de situatie. In deze fase realiseren slachtoffers zich dat er iets grondig mis is, maar ze weten niet wat er aan de hand is. Slachtoffers zoeken elkaar op voor steun en overleg.
In de derde fase, de besluitvormingsfase, hebben slachtoffers geaccepteerd dat ze in gevaar zijn en nemen ze, al dan niet bewust, een besluit waarmee ze hopen hun leven te kunnen redden. Slachtoffers zullen zich niet bewust zijn van deze verschillende fasen. Het kan seconden of zelfs (vele) minuten duren alvorens ze na de ramp tot actie overgaan, maar hoe lang het ook duurt, veel slachtoffers verklaren achteraf dat de tijd volkomen stil leek te staan.

Het profiel van een overlevende

Deze drie fasen verklaren nog niet wie een ramp overleeft en waarom. Ook Riply heeft daar geen pasklaar antwoord op. De mate van zelfredzaamheid, en daarmee de kans om een ramp te overleven, is afhankelijk van verschillende factoren waarbij de persoonskenmerken van een slachtoffer een cruciale rol spelen. Onder persoonskenmerken verstaat Riply het geheel van genetische aanleg, het karakter en fysieke kenmerken. Persoonskenmerken zijn een gegeven waar weinig aan te veranderen valt. Sommige mensen zijn op grond van genetische factoren meer stressbestendig dan anderen. Iemand die stressbestendig is zal beter in staat zijn om met acute stress om te gaan en kan onder extreme omstandigheden sneller en adequater handelen. Een optimistisch karakter en een flinke portie zelfvertrouwen dragen ook bij aan een grote mate van zelfredzaamheid. Dat fysieke kenmerken eveneens een rol spelen bij het vermogen tot zelfredzaamheid, ligt voor de hand.

Iemand die slecht ter been is, of ernstige gezondheidsklachten heeft zal meer problemen ondervinden om zichzelf in veiligheid te brengen. Naast deze factoren, waar geen of weinig invloed op uit te oefenen is, constateert Riply dat er nóg een factor is die van invloed is op zelfredzaamheid. Dat is de mate van kennis en/of ervaring waarover een slachtoffer beschikt en die bijdraagt aan zelfredzaamheid na een ramp. Dit is een gedeelde verantwoordelijkheid van burgers, werkgevers en overheid.
Burgers die weten hoe ze onder bepaalde omstandigheden moeten handelen hebben meer zelfvertrouwen als ze geconfronteerd worden met een ramp. Dat kan door bij voorbeeld de veiligheidsinstructies in het vliegtuig goed te lezen of te controleren waar de nooduitgangen zijn in de metro of hotel. Ook stelt Riply dat burgers risico's moeten beoordelen op basis van feiten en niet op emoties. Uit onderzoek blijkt bijvoorbeeld dat veel mensen zich ongerust maken over nucleaire ongevallen of ongevallen met chemische stoffen. Het risico op een brand in de eigen woning is echter vele mate groter. Toch wordt dit risico vaak (veel) te laag ingeschat. Met als gevolg dat nog steeds te weinig mensen rookmelders in hun woning hebben en er nog steeds teveel mensen door een woningbrand overlijden.
Werkgevers kunnen de zelfredzaamheid van medewerkers bevorderen door het houden van realistische evacuatie oefeningen. Dat betekent onder andere dat medewerkers geen persoonlijke bezittingen mee mogen nemen en per direct naar de nooduitgangen moeten gaan om zich in veiligheid moeten brengen. Bij de evaluatie van deze oefeningen zouden werkgevers zich ook (meer) bewust moeten zijn van de evacuatienormen die bij de bouw van het gebouw in acht genomen zijn. Riply noemt als voorbeeld dat na de aanslagen van 9/11 de ontruiming per etage gemiddeld een minuut duurde. Dat lijkt snel maar bleek twee keer langer dan de norm waarvan de bouwers waren uitgegaan.
De overheid ten slotte, heeft tot taak om burgers over risico's te informeren. Riply stelt dat goede overheidsinformatie consistent, gemakkelijk te begrijpen, specifiek, regelmatig herhaald, persoonlijk, accuraat en doelgericht is. Kernboodschap is dat mensen niet alleen moeten begrijpen welke risico's ze daadwerkelijk kunnen lopen, maar ook wat ze in een dergelijke situatie moeten doen en vooral: waarom ze dat moeten doen.

Groepsdynamiek

Niet iedereen heeft een koelbloedig, stressbestendig karakter. Sommige slachtoffers zijn na een ramp letterlijk en figuurlijk verlamd van angst. Van zelfredzaamheid, is dan geen sprake meer. Toch is er voor deze slachtoffers en slachtoffers die om wat voor reden niet mobiel zijn nog hoop. Riply noemt verschillende voorbeelden waaruit blijkt dat ook deze slachtoffers een ramp kunnen overleven. Dit dankzij het feit dat sommige mede-slachtoffers de rol van leiderschap op zich nemen. Ze weten met duidelijke instructies, geloofwaardigheid en kalm optreden zichzelf en andere slachtoffers in veiligheid te brengen.

Conclusie en beoordeling

Het antwoord op de vraag "wie overleeft een ramp en waarom" is niet eenduidig te beantwoorden. Persoonskenmerken van het slachtoffer, kennis en ervaring en de groepsdynamiek spelen in elk geval een belangrijke rol. Een meer algemene conclusie is dat kennis van het menselijk gedrag, zowel het individuele gedrag als dat in groepsverband, een randvoorwaarde is voor het bevorderen van zelfredzaamheid in het bijzonder en een integraal veiligheidsbeleid als geheel. Riply's boek geeft rampen een menselijk g ezicht door de persoonlijke getuigenissen van slachtoffers. Haar boek bevat daarnaast tal van interessante (onderzoeks-) feiten. Door de enorme hoeveel informatie en de wijze waarop ze deze presenteert is het boek niet echt toegankelijk voor een breed publiek. Voor beleidsmakers is het zonder meer een aanrader.

Het boek "*The Unthinkable. Who survives when disaster strikes-and why*" is uitgebracht door uitgeverij Crown Publishers, US (ISBN 978-0-307-35289-7).

Marieke Timmermann en Ragna Opten, *communicatieadviseurs Programma Burgernet*

BURGERNET Werkt!

27.000 burgers **leveren actieve bijdrage** aan veiligheid

Horen

Zien

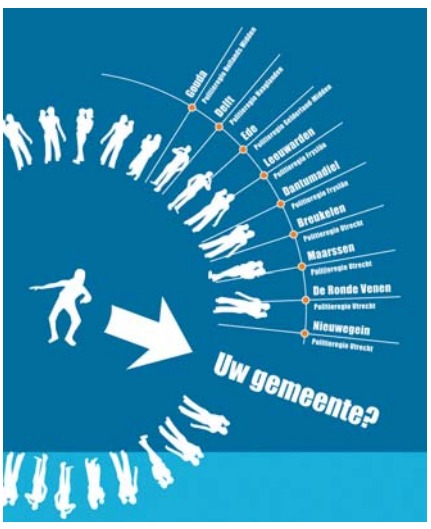
Bellen

Burgernet, een samenwerkingsverband tussen burgers, gemeente en politie, is een concrete vorm van de burgerparticipatie met als doel de veiligheid in de woon- en werkomgeving te bevorderen. En Burgernet werkt: inmiddels zijn er ruim 27.000 deelnemers, heeft de inzet ervan tot aanhoudingen en/of belangrijke informatie voor de opsporing geleid en is een intensieve samenwerking ontstaan tussen politie, gemeente en deelnemende burgers. Nu richt Burgernet zich nog specifiek op opsporing, maar het systeem is gereed voor een bredere inzet en heeft de potentie om een effectieve bijdrage te leveren aan crisisbeheersing.

Meerdere gemeenten en korpsen hebben inmiddels belangstelling voor de invoering van Burgernet. Wim Cornelis, burgemeester van pilotgemeente Gouda, begrijpt dit enthousiasme wel: 'De resultaten zijn positief en de animo ervoor onder de inwoners is groot. Burgers willen ook graag een actieve bijdrage leveren aan de veiligheid in hun woon- en werkomgeving en zien dit ook als een eigen verantwoordelijkheid. In Gouda hebben we nu 3312 deelnemers, een enorm hoge participatiegraad. Het geeft wel aan dat men hier een steentje wil bijdragen aan het veiligheidsgevoel. Wij hebben Burgernet ook opgenomen in het lokale integrale veiligheidsbeleid'.

Burgernet en crisisbeheersing

Cornelis ziet veel mogelijkheden voor Burgernet op multidisciplinair gebied:



'Het systeem – met zijn grootschalige uitbel en inbeldiensten – heeft de potentie om ook multidisciplinair ingezet te worden in de geïntegreerde meldkamer en op het niveau van de veiligheidsregio. De brandweer kan bijvoorbeeld bij een grote brand waarbij een gifwolk is vrijgekomen, Burgernet-deelnemers uit het getroffen gebied alarmeren en instructies geven. De GHOR/GGD kunnen deelnemers informeren over wat te doen bij een infectieziekteuitbraak in de gemeente. Of denk aan nutsbedrijven; als het waternet eruit ligt of de elektriciteit is afgesloten, kunnen zij de mensen op de hoogte houden van de ontwikkelingen. Belangrijk is wel dat Burgernetdeelnemers zelf aangeven dat zij ook voor andere (hulp) diensten willen worden ingezet envoorwaarde is een heel breed dekkend netwerk'. Hugo Vos, projectleider Burgernet politieregio Hollands Midden:'Het net kan goed worden uitgebreid voor preventieberichten of als alarmeringssysteem. In de gemeente Jacobswoude is bij een bomruiming gewerkt met SMS en met tijdelijke deelnemers, alleen voor dit incident. Op deze manier zijn snel veel mensen geïnformeerd. Het bereik is hierbij groter dan alleen het Burgernetwerk. In de praktijk blijkt namelijk dat deelnemers een oproep ook delen met familieleden en mensen in de directe omgeving'.

Advies landelijke invoering

De Stuurgroep Burgernet heeft de ministers van BZK en Justitie geadviseerd om Burgernet (gefaseerd) landelijk in te voeren. Ook is daarbij aanbevolen het soortgelijke initiatief voor burgerparticipatie SMS Alert te integreren in Burgernet. Deze integratie moet leiden tot een eenduidig aanbod van diensten door de Nederlandse politie onder de naam Burgernet.

Meer weten: www.burgernet.nl

Burgernet in praktijk

De centralist van de meldkamer van de politie start, na een melding van bijvoorbeeld een inbraak of een vermist kind, een Burgernetactie op. Deelnemers krijgen een ingesproken of tekstbericht via de (mobiele) telefoon of met het verzoek uit te kijken naar een duidelijk omschreven persoon of voertuig. Als Burgernetdeelnemers de persoon of het voertuig zien dat voldoet aan het signalement, bellen ze via een gratis nummer direct met de meldkamercentralist van de politie. Naar aanleiding van de verkregen informatie stuurt de centralist de politie aan. Alle deelnemers ontvangen na afloop van de Burgernetactie een bericht over de resultaten van de actie. Van november 2008 t/m mei 2009 is Burgernet succesvol beproefd in Gouda (politieregio Hollands Midden), Delft (politieregio Haaglanden), Ede (politieregio Gelderland Midden), Leeuwarden en Dantumadeel (politieregio Fryslân), Breukelen, Maarssen, De Ronde Venen en Nieuwegein (politieregio Utrecht).

Frank Kalshoven en Jenny Kossen,
directeur respectievelijk kaartenmaker bij De Argumentenfabriek

Voorzag u in 2006 dat de terugval van de Amerikaanse huizenmarkt het failliet van IJsland zou veroorzaken? Bedacht u in augustus 2007 dat de afschrijvingen op Amerikaans schuldpapier zouden leiden tot de nationalisatie van ABN AMRO en Fortis Bank Nederland? Wist u na de val van Lehman Brothers dat de wereldeconomie dit jaar voor het eerst in zestig jaar zou krimpen?

Een instabiele wereld vereist een lenige geest

De financieel-economische crisis en de gevolgen voor Nederland

De kredietcrisis, begonnen op de Amerikaanse huizenmarkt, heeft grote gevolgen voor Nederland. Wat een jaar geleden niet voor mogelijk werd gehouden, is vandaag realiteit.
Het verloop van de crisis is moeilijk te voorspellen, en dat geldt ook voor de gevolgen op nationaal niveau. Beleidsmakers en politici moeten zich hier echter wel op voorbereiden want in de toekomst wordt van hen een verstandige beleidsreactie verwacht. Om dat te kunnen doen is vooral lenigheid van geest nodig. Die lenigheid kan getraind worden door na te denken over toekomstbeelden.
Een groep gezaghebbende deskundigen op het gebied van onder meer economie, veiligheid en sociale verhoudingen heeft daarom in het vroege voorjaar van 2009 de gevolgen van een drietal mogelijke – niet de meest waarschijnlijke – gebeurtenissen verkend: 'De val van de dollar', 'Grondstof-shoppen' en 'Breuklijnen in Europa'. Deze verkenningen hebben een aantal inzichten opgeleverd die de moeite waard zijn, ook nu het met de gevolgen van de crisis vooralsnog lijkt mee te vallen.
In opdracht van de Secretarissen-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken heeft de Argumentenfabriek het denkproces van de deskundigen begeleid en de mogelijke internationale en nationale gevolgen van de drie gebeurtenissen gevisualiseerd op Informatiekaarten. Hieronder schetsen we de hoofdlijnen van het kaartenboek dat hierover is verschenen.

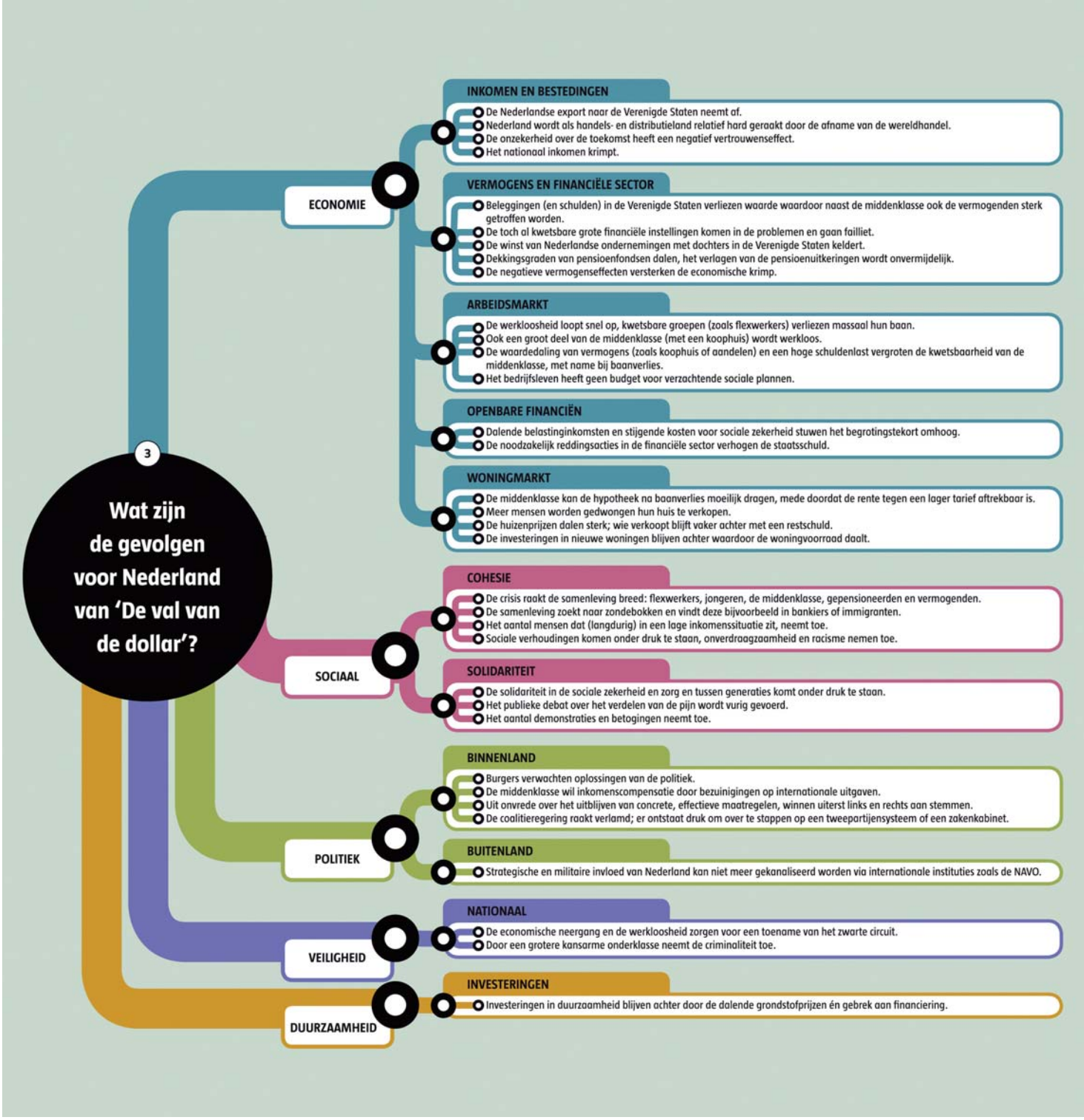
Gebeurtenissen

Met de deskundigen is eerst nagedacht over mogelijke internationale gebeurtenissen die zich kunnen voordoen in een wereld die zowel financieel-economisch als politiek minder stabiel is dan nu. Uit deze gebeurtenissen hebben de deskundigen er drie gekozen die zij het meest relevant vonden om te doordenken op hun belangrijkste internationale, maar vooral ook nationale gevolgen. Dit zijn 'De val van de dollar', 'Grondstof-shoppen' en 'Breuklijnen in Europa'.
Een val van de dollar kan bijvoorbeeld ontstaan wanneer het buitenland de Amerikaanse schuld niet langer kan of wil financieren. Bij 'grondstof-shoppen' geven snelgroeiende landen een extra impuls aan het inkopen van grondstoffen en grondstofleveranciers in de rest van de wereld. Breuklijnen in Europa kunnen ontstaan als landen langs de periferie van de Europese Unie (EU) in betalingsproblemen komen en onvoldoende ondersteund worden door de overige EU-landen.

Nationale gevolgen

Voor elk van de drie gebeurtenissen is steeds één variant van de internationale en nationale gevolgen volledig doordacht, als een consistent geheel van oorzaak en gevolgen. Op elk moment kan een interventie of een andere gebeurtenis de loop van deze gevolgen beïnvloeden. De gevolgen zouden dan anders zijn.

Het verkennen van de nationale gevolgen van de drie gebeurtenissen levert een aantal inzichten op. Zo blijkt Nederland bovengemiddeld gevoelig voor internationale veranderingen. Dit komt door de sectorale opbouw van de Nederlandse economie (een relatief grote financiële en exportsector) en omdat Nederland veel geld heeft geïnvesteerd in het buitenland. Die investeringen lopen via de pensioenfondsen en via directe buitenlandse investeringen van het bedrijfsleven. De waarde van deze investeringen komt door economische instabiliteit >>>



Figuur: Visualisatie gevolgen voor Nederland van val dollar

onder druk te staan, bijvoorbeeld door de stijging van de wisselkoers van de euro of door sterke economische krimp in de landen waar Nederland heeft geïnvesteerd. Een economische neergang komt steeds als eerste terecht bij de sociaal-economisch zwakkere groepen. Zo worden allochtonen harder geraakt door de crisis dan autochtonen, de (veelal jonge) flexwerkers lopen meer risico dan mensen met een vast contract. Naarmate de crisis heviger en langdurig wordt, worden ook de midden- en hogere inkomens geraakt. Wanneer zij hun baan verliezen daalt hun inkomen sterk terwijl hun schuldverplichting (zoals een hypotheek) overeind blijft. Dit kan leiden tot meer gedwongen verkoop van woningen en dalende huizenprijzen. Mensen zullen dus na verkoop vaker met een restschuld achterblijven. Dit negatieve vermogenseffect wordt nog eens versterkt doordat ook de pensioenen en beleggingen minder waard worden.

Verdergaande economische en politiek instabiliteit kent dus vele verliezers. Omdat het sociale vangnet de verliezen van mensen niet kan compenseren en misschien omwille van de financierbaarheid zelfs verkleind moet worden, kan de onvrede over de overheid toenemen. Hierdoor wordt de populariteit van politieke partijen buiten het centrum vergroot.

De crisis en zijn gevolgen kunnen eveneens leiden tot spanningen. Bijvoorbeeld door het ontstaan van grondstofschaarste. Waar de spanningen precies ontstaan is op voorhand onduidelijk, maar de deskundigen wijzen expliciet op een mogelijke toename van het anti-migrantensentiment onder de sociaal-economisch zwakke groepen.

Tot slot

We leven in turbulente en onvoorspelbare tijden. Wat een jaar geleden ondenkbaar leek, is nu realiteit. Hoe de wereld er over een jaar uitziet, valt moeilijk te zeggen. Door voortdurend na te denken over onwaarschijnlijke gebeurtenissen die, als ze zich toch voordoen, een grote impact hebben, worden verrassingen kleiner en komen adequate beleidsreacties een stap dichterbij. In een instabiele wereld hebben beleidsmakers een lenige geest nodig.

Meer informatie: www.argumentenfabriek.nl

Het kaartenboek kan worden besteld via Alice.focke@minbzk.nl.

Met een verruimde blik terug naar de actualiteit

Mw. ing. Roos M. van Erp-Bruinsma,
secretaris-generaal ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De omgevingsverkenningen zijn te plaatsen in het licht van een sterk veranderende wereld. Het zijn verkenningen van hoe de wereld er uit zou kunnen zien, mocht deze zich in een richting ontwikkelen van verminderde politieke en financieel-economische stabiliteit.

Door stil te staan bij mogelijke ontwikkelingen zijn wij beter in staat maatschappelijke trends en ontwikkelingen te herkennen, zodat we deze tijdig kunnen ombuigen en aanwezige kansen kunnen benutten.

In de omgevingsverkenningen laten deskundigen, met zeer diverse achtergronden, ons zien hoe de wereld er onder heel andere omstandigheden uit zou kunnen zien en wat dit voor Nederland zou betekenen. Wat kan er gebeuren als de dollar valt? Wat betekent het voor ons land als grondstofvoorraden in handen van één speler komen? En wat zijn de gevolgen voor Nederland als één of meerdere lidstaten zich zouden distantiëren van de Europese Unie?

De omgevingsverkenningen zijn niet bedoeld om zaken te voorspellen. Ze zijn bedoeld om maatschappelijke signalen en veranderingen eerder te kunnen herkennen. In onze samenleving vinden er regelmatig onverwachte gebeurtenissen plaats. We zijn dan snel geneigd om ons eigen gelijk op te zoeken, terwijl het opsporen van je ongelijk zeker zo nuttig en leerzaam kan zijn.

We hebben met elkaar aan de omgevingsverkenningen gewerkt op een manier die niet alleen buitengewoon inspirerend was maar waarmee we ook in de toekomst complexe vraagstukken kunnen verkennen en in een breder internationaal en nationaal perspectief kunnen plaatsen. Zo kunnen we met een verruimde blik naar de actualiteit terugkeren.

Kritiek op griepcommunicatie: terecht of onterecht?

De afgelopen weken was de overheidscommunicatie over griep het gesprek van de dag. In alle kranten gaven deskundigen tips over het gebruik van social media, in de meeste actualiteitenprogramma's op tv kwam de antiprik-lobby aan het woord en op internet vierden geruchten en complottheorieën over het vaccin hoogtij. De overheids-communicatie zou hopeloos achterlopen en geen grip hebben op de berichtgeving.

Maike Delfgaauw,
adviseur risico- en crisiscommunicatie Nationaal Crisiscentrum
Marian Byvanck,
coördinator griep-communicatie VWS

Sinds de uitbraak van de Nieuwe Influenza A H1N1 is er kritiek op het communicatiebeleid van het ministerie van Volksgezondheid, Welzijn en Sport (VWS). En dat is goed, omdat die kritiek de communicatie helpt te verbeteren en daarnaast een aantal dingen duidelijk maakt. Dat communiceren over onzekerheid lastig is; dat de (informatie)maatschappij snel verandert en je daar als overheid goed op toegerust moet zijn; dat we als overheid geen grip op de berichtgeving (moeten willen) hebben; dat de overheid kampt met het feit dat haar deskundigheid en autoriteit in twijfel worden getrokken en dat ook de autoriteit en deskundigheid van wetenschappers door het publiek nogal eens in twijfel wordt getrokken.

Maar is die kritiek nu terecht?

Laten we eens kijken naar de resultaten van de communicatie-aanpak van VWS.
Deze griep is de eerste dreiging waarbij de overheid gestructureerd en frequent onderzoekt wat publiek en media vinden (elke 14 dagen een publiekspeiling, wekelijkse blog-analyses en media-analyses). Die onderzoeksgegevens worden gebruikt bij de vormgeving en aanscherping van publiekscommunicatie en woordvoering. De analyses wijzen tot nog toe uit dat de traditionele media behoorlijk evenwichtig berichten. Op blogs is veel echo van de traditionele media maar daarnaast veel aandacht voor geruchten en complot-theorieën. Daardoor ontstaat er een soort pseudo-deskundigheid en weten deze mensen massa te creëren op internet. Als je het kritisch onderzoekt, blijken er echter slechts een paar bronnen te zijn, die vooral naar elkaar doorlinken.

Nederlanders hebben vertrouwen in de informatie-voorziening en maatregelen

Uit de publiekspeiling, die wordt verricht door een onafhankelijk onderzoeksbureau Market Response,

blijkt dat het vertrouwen van het publiek in de informatievoorziening (70%) en de maatregelen (80%) van de overheid op 9 en 10 november flink is gestegen ten opzichte van eind oktober, terwijl we toen op het – voorlopig – hoogtepunt van de geruchtenstorm en kritiek op de communicatie zaten. De vaccinatiebereidheid lijkt zowel in de peilingen als in de daadwerkelijke opkomst ten minste op het niveau van de seizoensgriep te liggen (75% van de doelgroep). Dat is internationaal gezien een zeer hoge vaccinatiegraad.

Griepcommunicatie en social media

Verschillende deskundigen gaven VWS via de traditionele media tips over het gebruik van social media (denk aan Twitter, Hyves, blogs, fora). Hoewel VWS het merendeel van de geadviseerde zaken al doet, kan dat inderdaad beter. De uitdaging is, om als overheid actiever te participeren in de discussies op internet en dat efficiënt te doen, gezien de hoeveelheid blogs en fora (je kunt niet overal op reageren) en effectief (welk resultaat bereik je ermee?). De ervaring bij de griepcommunicatie is, dat je als overheid van het (kritische) forum wordt geweerd, tenzij je écht inhoudelijk meepraat. In het geval van een medisch onderwerp is daarvoor deskundigheid nodig die je van een webredacteur of extern webcare team niet kunt verwachten. De inhoudsdeskundigen zijn juist nu bezig met onderzoek, organisatie en uitvoering van de vaccinatie. Wat wel meer zou kunnen gebeuren is je als overheid minder als zender te gedragen, de inhoud meer naar mensen toe te brengen door de interactiviteit te verhogen en bestaande informatie op plaatsen te brengen waar zich discussie afspeelt. Daarnaast leert onderzoek dat je als overheid weinig kan doen tegen complottheorieën, je bent als afzender immers per definitie onbetrouwbaar voor degenen die in die theorieën geloven.

Wat willen we eigenlijk bereiken?

Het doel van de communicatie-inspanningen van VWS, via welk medium dan ook, is niet om de tegengeluiden te doen verstommen. Integendeel: het doel is om mensen voldoende informatie te geven om griep zoveel mogelijk te voorkomen, symptomen te herkennen en zo snel mogelijk beter te worden en om informatie voor vaccinatiedoelgroepen zodanig aan te bieden dat ze hun keuze om zich wel of niet te laten vaccineren goed kunnen maken. Tegengeluiden horen daarbij. Dat laat onverlet dat we met de griepcommunicatie moeten blijven inspelen op de informatiebehoefte van mensen.

ZO HOUDEN WE
GRIP OP GRIEP

Ana Lidia Aneas Moyano,
senior communicatie adviseur EU FloodEx
(analidia.aneas@minbzk.nl)

FLOODEX: internationale bijstand tijdens ergst denkbare overstroming

Van 21 tot en met 25 september vond de internationale veldoefening EU FloodEx 2009 in Noord-Holland Noord plaats, tiidens welke het ontvangen van en het samenwerken met inkomende internationale bijstand bij een grootschalige overstroming werd beoefend. De oefening was georganiseerd door het LOCC namens het ministerie van BZK in samenwerking met de Veiligheidsregio Noord-Holland Noord. Ruim 30 organisaties uit binnen en buitenland hebben samengewerkt aan de voorbereidingen en realisatie van EU FloodEx 2009. Het totaal aantal deelnemers per dag was 925, waaronder 300 figuranten en Lotus-slachtoffers, 294 internationale deelnemers en 110 hulpverleners uit Regio Noord-Holland Noord, waaronder Reddingsbrigade.

Media aandacht – VIP programma
De belangstelling vanuit de media was groot. Ruim 75 journalisten uit binnen en buitenland, waaronder BBC, ZDF, NOS, diverse RTV's, dag- en vakbladen, versloegen de in scene gezette watersnoodramp. Ruim 70 VIP's uit binnen en buitenland konden de oefeningen rondom het Alkmaardermeer vanuit boot en helikopter aanschouwen. Van dichtbij hebben zij zich kunnen inleven in het werk van een hulpverlener tijdens extreme omstandigheden, zoals diverse evacuaties op kleine en grote schaal, de befaamde reddingsacties van daken en de ontsmetting van slachtoffers.

Tijdens het middagprogramma presenteerde Sir Michael Pitt, voormalig voorzitter van de onderzoekscommissie van de 'lessons learned' van de overstromingen in Groot-Brittannië (2007) en sprak Pia Bucella, directeur Civil Protection Unit van de Europese Commissie over de toegevoegde waarde van het EU Civil Protection Mechanism. De resultaten van TMO (Tasforce Management Overstromingen) werden door Ruurd Reitsma, voormalig Programma Manager TMO gepresenteerd.

Evaluatie
Na een intensieve training in de vorm van de Masterclass Evaluatoren, eerder dit jaar mochten 20 enthousiaste internationale evaluatoren aan de slag. Vijf intensieve dagen in het veld hebben geleid tot een grote hoeveelheid observaties. De observaties worden geanalyseerd en gebundeld in een rapport. Eind dit jaar verschijnt de bijbehorende evaluatie DVD.

Deelnemersveld EU Floodex 2009

Duitsland (115 team members)
- BBK Federal Office of Civil Protection and Disaster Assistance
- Federal Police
- German Life Saving Association
- Technisches Hilfswerk (THW)

Estland (26 team members)
- Estonian Rescue Board
- West Estonian Rescue Services Centre

European Commission (11 team members)
- EU Coordination Team
- EU Monitoring and Information Centre

Polen (20 team members)
- State Fire Service

United Kingdom (118 team members)
- Cabinet Office
- Hereford and Worcester Fire and Rescue Service

Nederland (290 team members)
- Agentschap Telecom
- Dutch Amateur Radio Emergency Service (DARES)
- Hoogheemraadschap Hollands Noorderkwartier
- Korps Landelijke Politiediensten
- Landelijk Operationeel Coördinatie Centrum
- Koninklijke Marechaussee
- Ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Defensie, Verkeer en Waterstaat, Volksgezondheid, Welzijn en Sport, Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
- Nationaal Crisis Centrum
- Nederlands Instituut Fysieke Veiligheid
- NIFV
- Reddingsbrigade
- Schiphol
- USAR.nl
- Veiligheidsregio Noord-Holland Noord


od Rescue
Team
www.rnli.org.uk
Lifeboa


DEMAG
V 42
INCIDENT RESPONSE UNIT


German Federal Agency
for Technical Relief
THW
DLRG
WATER RESCUE
DLRG
WATER RESCUE

Nationaal crisis- en veiligheidsbeleid in 2010
kernpunten begroting BZK

Op Prinsjesdag presenteerde het Kabinet de begroting voor 2010. Hieronder de kernpunten op het terrein van nationale veiligheid en crisisbeheersing uit de BZK-begroting.

Algemene doelstelling van het nationaal crisis- en veiligheidsbeleid is het voorkomen van en prepareren op dreigingen tegen de nationale veiligheid en zorgen dat burger, bedrijfsleven en overheids-organisaties goed voorbereid zijn op mogelijke crises.

Een eerste, daarvan afgeleide operationele doelstelling is het systematisch identificeren en beoordelen van mogelijke dreigingen en het in kaart brengen en waar nodig versterken van de strategische capaciteiten die nodig zijn om de dreigingen op de nationale veiligheid te voorkomen dan wel om er mee om te gaan. Daartoe worden de volgende instrumenten ingezet:

- Medio 2010 wordt de derde Nationale Risicobeoordeling (NRB) aangeboden aan de Tweede Kamer.
- Het ontwikkelen van scenario's van de verschillende dreigingen op de nationale veiligheid. Bestaande scenario's worden geactualiseerd en nieuwe ontwikkeld voor de thema's: digitale onveiligheid, internationaal georganiseerde criminaliteit, economische onveiligheid, natuurbrand en terrorisme.
- Met de vitale sectoren worden afspraken gemaakt over de continuïteit van de levering van vitale producten en diensten en waar nodig worden waakvlamovereen-komsten afgesloten. Met voorrang is hierbij aandacht voor de continuïteit van elektriciteit en ICT.
- De zelfredzaamheid van de burger zal verder worden versterkt. Zo wordt de burger geïnformeerd over de handelings-perspectieven bij de verschillende typen van dreigingen, o.a. via Denk Vooruit. Ook worden pilots gehouden over hoe burgerparticipatie verder kan worden uitgewerkt.
- Het ontwikkelen van landelijke strategieën voor de verdeling van schaarste voor de thema's verschuivende machts-verhoudingen en aanpassing economische structuren.
- De strategische samenwerking tussen de veiligheidsregio's, de vitale sectoren en de rijksoverheid wordt gecontinueerd in het Strategisch Overleg Vitale Infrastructuur (SOVI).
- Het bijdragen aan de onderhandelingen over en de uitwerking van het Europese programma voor de bescherming van vitale infrastructuur (EPCIP). Daarnaast wordt mogelijke Europese vitale infra-structuur geïdentificeerd en aangemerkt in Nederland.
- De uitvoering van het actieplan van de Europese Commissie om de weerbaarheid van de Europese Unie en haar lidstaten tegen Chemische, Biologische, Radio-actieve of Nucleaire incidenten (CBRN) te vergroten.
- Het bijdragen aan de onderhandelingen over en uitwerking van een EU-brede risico-analyse, met aandacht voor preventie en met het oog op de versterking van de regionale samenwerking, conform de NRB in Nederland.
- Het versterken van de landelijke aanpak van veiligheidsregio's met betrekking tot de bescherming van vitale infrastructuur en de continuïteit tijdens grieppandemie.
- Het ontwikkelen van een trendrapportage in het kader van ICT en Veiligheid en de beleidsaansturing van de samenwerking op het gebied van security.
- Het financieel en beleidsmatig bijdragen aan het implementatietraject van het programma Intensivering Civiel-Militaire Samenwerking (ICMS) gericht op de verdere samenwerking met de defensieorganisatie ten behoeve van de nationale veiligheid.
- Het verder uitwerken van de "nafase" met aandacht voor de deelprocessen "opvang en zorg voor getroffenen" en "herstel en wederopbouw", op basis van de aanbevelingen van de Taskforce Management Overstromingen (TMO) uit 2009. Daarbij zal het eerder ontwikkelde Modelplan Nafase worden herzien.
- Samen met het ministerie van VROM wordt een grootschalige nucleaire oefening voorbereid en gedraaid. Tevens worden samen met de Veiligheidsregio Zuid-Limburg voorbereidingen getroffen voor "Voyager II in 2011".

Een tweede operationele doelstelling is een effectieve nationale crisisresponsorganisatie voor de aansturing van crisisbeheersing. Daartoe worden de volgende instrumenten ingezet:

- De verdere doorontwikkeling van de crisisstructuur op rijksniveau: een rijksbrede één-loketfunctie voor crisismeldingen, een verbeterde gezamenlijke advisering van ministers en kabinet, een duidelijk producten- en dienstenaanbod richting de crisispartners, en interdepartementaal opleiden, trainen en oefenen (kennis en competenties).
- Inzet van ICT-voorzieningen om informatie-uitwisseling te optimaliseren.
- Het implementeren, evalueren en aanpassen van het Nationaal Handboek Crisisbesluitvorming, de landelijke operationele staf en het Nationaal Crisisplan.
- Een continuering van de ontwikkeling van het instrument risicosignalering en alertering.

De aanslag op Koninginnedag was een eenmansactie van Karst T., waarvoor hij slechts enkele voorbereidingen had getroffen. Zeer waarschijnlijk heeft hij met zijn zwarte Suzuki Swift de bus van de Koninklijke familie willen raken. Bij de gewelddadige actie kwamen acht mensen, waaronder de dader, om het leven. Negen anderen raakten ernstig gewond.

Aanslag Koninginnedag was eenmansactie

Het onderzoek door de Nationale Recherche van het Korps landelijke politiediensten (KLPD) en ook de gedragsdeskundige analyse door het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP) kunnen door de dood van Karst T. geen volledig zicht geven op zijn bedoelingen en motieven.

Het is aannemelijk dat Karst T. niet heeft geweten dat er mensen op de kruising stonden op het moment dat hij vanaf de Bosweg vertrok voor zijn dodemansrit. Het is ook niet vastgesteld dat hij, tijdens zijn rit over de Jachtlaan, het publiek op de kruising heeft gezien. Hoewel hij een aantal malen heeft geclaxonneerd, nam hij op geen moment snelheid terug, noch blijkt uit technisch onderzoek dat hij heeft geremd.

In het onderzoek van de Nationale Recherche lag de nadruk op het uitsluiten van vele denkbare scenario's over de toedracht van het gewelddadige incident. Naast het voorkomen van eventuele vervolgaanslagen was het vergaren van bewijs over het incident zelf een belangrijke prioriteit.

Onder gezag van het Landelijk Parket heeft het onderzoek door de Nationale Recherche zich gericht op een reconstructie van de gewelddadige actie, de voorbereiding en het motief van de dader. Parallel hieraan werd samen met de regiopolitie hulp aan slachtoffers en nabestaanden verleend.

Bewust tegen de bus

Toen het voertuig tegen het monument 'de Naald' tot stilstand was gekomen sprak T. met opsporingsambtenaren en een ambulanceverpleegkundige. Hij verklaarde meermalen zijn actie bewust te hebben uitgevoerd. Uit het onderzoek is gebleken dat de auto door de aanrijding met de hekken en het publiek van richting veranderde en tegen 'de Naald' tot stilstand kwam. Uit technisch onderzoek is gebleken dat de auto, gedurende de gehele rit bestuurbaar is gebleven. Wanneer de auto in botsing was gekomen met de bus van de Koninklijke familie zouden de inzittenden lichte tot zware verwondingen hebben opgelopen, afhankelijk van de snelheid van de auto en de precieze hoek van de inslag.

Door de Nationale Recherche is onderzocht of Karst T. aanhanger was van een bepaalde politieke of levensbeschouwelijke overtuiging die hem tot zijn daad kon hebben gedreven. Politiek of levensbeschouwelijk actief was hij nooit. Het is onwaarschijnlijk dat hij vanuit een bepaalde bestaande ideologie of levensbeschouwing tot zijn daad kwam. Ook zijn er geen aanwijzingen gevonden, dat hij een extreme aversie tegen het Koninklijk Huis had.

Geestesgesteldheid

Het NIFP heeft, in opdracht van het Openbaar Ministerie een gedragsdeskundige analyse gedaan naar de geestesgesteldheid van Karst T. om meer inzicht te krijgen in de gebeurtenissen en vast te stellen of er voor of tijdens het incident bij Karst T. een eventuele psychiatrische stoornis vastgesteld of uitgesloten kon worden. Op basis van dit onderzoek kon bij Karst T. geen psychiatrische stoornis worden vastgesteld, niet in zijn voorgeschiedenis en ook niet ten tijde van het incident.

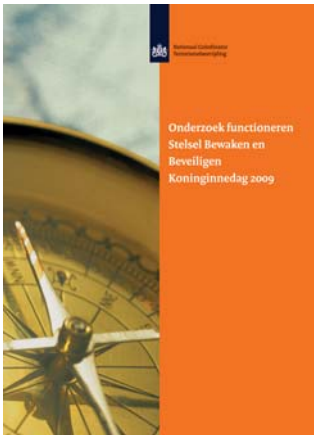
(bron: Persbericht Landelijk Parket, 4 september 2009)

Nora Timmermans,
senior beleidsmedewerker Eenheid Bewaken en Beveiligen (EBB), NCTb

Op zoek naar het evenwicht

De juiste balans

tussen feestelijkheid en veiligheid



De Nationaal Coördinator Terrorismebestrijding heeft het feitelijk functioneren van het stelsel bewaken en beveiligen bij de beveiliging van de koninklijke familie in de aanloop en tijdens Koninginnedag 2009 onderzocht. Eén van de belangrijkste aanbevelingen van zijn onderzoek is dat structurele coördinatie ten behoeve van samenhang en afstemming tussen alle betrokken partijen in het proces van bewaken en beveiligen rond nationale evenementen noodzakelijk is en moet worden versterkt.

Koninginnedag kent traditiegetrouw een feestelijk en open karakter. Talloze organisaties werken daarbij intensief samen om te zorgen voor een feestelijke en veilige viering voor zowel de koninklijke familie als het publiek. Het kabinet hecht er aan dat het open en feestelijke karakter van dit soort evenementen niet wezenlijk verandert. Het is belangrijk om te beseffen dat nooit alle risico's zijn uit te sluiten. Beveiliging krijgt na de tragische gebeurtenissen van Koninginnedag 2009 een meer prominente rol, zonder daarbij het feestelijke karakter al te zeer in te perken. De Nationaal Coördinator Terrorismebestrijding zet zich in om de juiste balans te vinden tussen feestelijkheid en veiligheid. De zoektocht naar balans wordt bepaald door drie elementen: het gegeven dat absolute veiligheid niet bestaat, het inzicht in risico's en de spanning tussen beveiliging en andere belangen.

Absolute veiligheid bestaat niet

Absolute veiligheid bestaat niet. Veiligheid is altijd de uitkomst van een afwegingsproces waarin per definitie een aantal risico's moet worden geaccepteerd. Anders zou het leiden tot excessieve maatregelen en wordt bovendien voorbij geschoten aan het doel van beveiligen: namelijk het ongestoord en zo veilig mogelijk kunnen functioneren ondanks dreiging of risico. Het zou toch ondenkbaar zijn om de gouden koets op Prinsjesdag te vervangen door een geblindeerde wagen, of de Tweede Kamer fysiek af te sluiten voor publiek?

Proportionaliteit van de maatregelen staat daarom altijd centraal bij beslissingen over welke maatregelen noodzakelijk zijn. Het besluit welke risico's aanvaardbaar zijn, is lastig te duiden en niet uitputtend te beschrijven. Ervaring, kennis en een compleet beeld van de situatie zijn de basis voor het nemen van deze besluiten.
In nauwe samenwerking met het lokaal bevoegd gezag zal de Nationaal Coördinator Terrorismebestrijding voortaan bij nationale evenementen dan ook, nadrukkelijker dan tot dusverre, een rol spelen bij de beslissing welke risico's geaccepteerd worden en welke niet. In de huidige verdeling van beveiligingstaken en verantwoordelijkheden verandert niets, wel in de wijze waarop daarvan gebruik wordt gemaakt.

Minder voorstelbare risico's

Dreiging en risico zijn leidend bij beslissingen over beveiliging. Beveiligingsmaatregelen worden immers niet voor de bühne genomen maar omdat er sprake is van een dreiging of een risico. Het inzicht in alle

mogelijke risico's is een bepalend element in bewaken en beveiligen. Dit terrein is relatief nieuw en continu in ontwikkeling. Het is vrijwel onmogelijk om alle potentiële risico's in kaart te brengen. Wie had gedacht dat een journalist zijn schoen zou werpen naar de Amerikaanse president? Of dat iemand te paard een stoet doorbreekt? Toch zal meer dan voorheen ook rekening moeten worden gehouden met risico's en scenario's die we tot nu toe als minder of niet voorstelbaar hadden geacht. De Nationaal Coördinator Terrorismebestrijding zal daarom samen met de politiekorpsen en de inlichtingen- en veiligheidsdiensten een landelijke lijst opstellen van mogelijke risico's en scenario's. Op basis van deze lijst kunnen beveiligingsmaatregelen worden getroffen die ook weerstand bieden tegen die risico's.

Beveiliging versus andere belangen

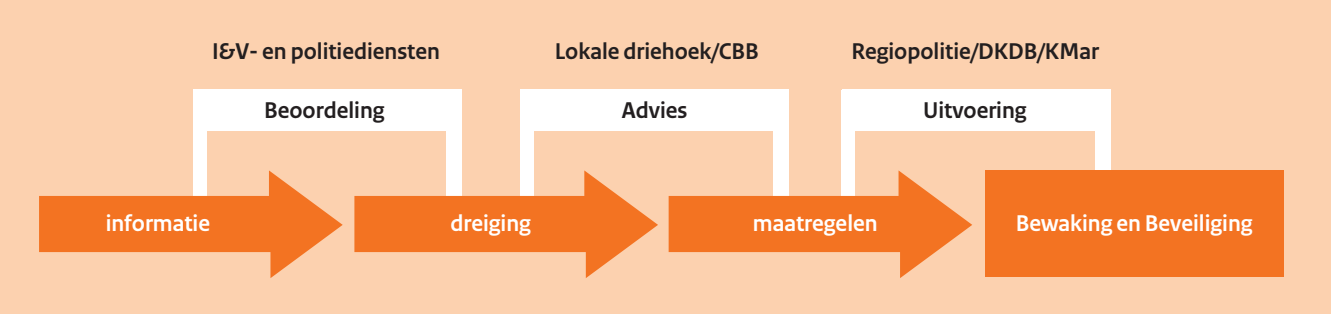
Beveiliging is erop gericht om met zo min mogelijk impact zoveel mogelijk weerstand te creëren tegen de dreiging of het risico. Het derde bepalende element bij bewaken en beveiligen is dat beveiliging vaak op gespannen voet staat met andere belangen. Voor politici is het bijvoorbeeld belangrijk om toegankelijk te zijn voor mensen en aandacht te trekken voor hun activiteiten. Dit leidt automatisch tot veiligheidsrisico's: immers iedereen weet waar ze zich bevinden.
Beveiligingsmaatregelen hebben altijd een impact op de te beveiligen persoon of object en diens omgeving. Vooral de meer ingrijpende beveiligingsmaatregelen leggen beperkingen op. Het komt in de praktijk geregeld voor dat aan de voorgenomen beveiliging aanpassingen worden gedaan om het ongehinderd functioneren van de bedreigde persoon voorop te stellen of andere belangen voor te laten gaan.
Bij nationale evenementen zie je vaak dat er veel andere belangen spelen die de beveiliging (negatief) kunnen beïnvloeden, zoals de aanspreekbaarheid van de Koningin voor het publiek. Maar ook dat er ongestoord verslag kan worden gedaan van de dag. Bovendien geldt dat veel verschillende partijen dit soort belangen hebben en hierover zelfstandig beslissingen nemen. Deze beslissingen kunnen vaak op zichzelf geen kwaad, maar bij elkaar opgeteld kan dit mogelijk wel leiden tot een set van aanpassingen die het niveau van de beveiliging op onacceptabele wijze beïnvloeden. Het is daarom van groot belang dat alle voorgenomen aanpassingen in zijn geheel worden beschouwd en dat creatief wordt gezocht naar alternatieve maatregelen om de dreiging weg te nemen of het risico af te dekken. In de toekomst worden bij nationale evenementen de afwegingen tussen veiligheid en andere belangen integraal op het niveau van het lokaal bevoegd gezag en de Nationaal Coördinator Terrorismebestrijding gemaakt.

De juiste balans

Samenwerken, overleg, delen van informatie en een open houding zorgen ervoor dat de juiste balans wordt gevonden tussen feestelijkheid en veiligheid. Bewaken en beveiligen is dan ook een dynamisch beleidsterrein dat zich blijft ontwikkelen en waarop continu afwegingen moeten worden gemaakt. Het is van belang om te blijven zoeken naar nieuwe manieren om te beveiligen en dreigingen het hoofd te bieden. De innovatie van beveiligingstechnieken heeft een hoge prioriteit bij de Coördinator Bewaking en Beveiliging. Maar er wordt ook naar andere manieren gezocht om het risico te reduceren of de dreiging weg te nemen. Een voorbeeld daarvan is de *Zeker van je Zaak-training* die de NCTb heeft ontwikkeld om het beveiligingsbewustzijn bij medewerkers van bedrijven en instellingen te versterken. Veel winst valt te halen uit alerte medewerkers die zich bewust zijn van de risico's en verdachte situaties. Dat vermindert de kans op een overmaat aan beveiliging en draagt bij aan een juiste balans tussen feestelijkheid en veiligheid.

Het onderzoeksrapport naar het functioneren Stelsel Bewaken en Beveiligen Koninginnedag 2009 is te vinden op www.nctb.nl.

Figuur: Schematische weergave proces bewaken en beveiligen



Onderzoek Inspectie OOV
Koninginnedag 2009 Apeldoorn

drs J.N.M. Groot MBA (projectleider) en E.P.H. Moonen,
beiden senior inspecteur bij de Inspectie Openbare Orde en Veiligheid

Naar aanleiding van het dramatische incident op Koninginnedag 2009 verzocht het college van burgemeester en wethouders van Apeldoorn de Inspectie Openbare Orde en Veiligheid (Inspectie OOV) een feitenonderzoek te verrichten naar het aspect openbare orde en veiligheid, zowel in de voorbereiding als tijdens de uitvoering van Koninginnedag 2009. Doelstelling van het onderzoek was om vanuit feiten en bevindingen tot een eenduidig beeld van de gebeurtenissen te komen. Daarnaast moest het rapport aangeven in hoeverre er verschillen waren tussen beslissingen, plannen et cetera in de voorbereiding van het evenement en de daaropvolgende uitvoering en de afhandeling van het incident.

Voorbereiding Koninginnedag

Bij de voorbereiding van Koninginnedag 2009 in Apeldoorn hebben veel organisaties in het kader van openbare orde en veiligheid samengewerkt. Naast gemeentelijke en regionale veiligheidsorganisaties in Noord- en Oost-Gelderland waren de DKDB, de KMar en de NCTb betrokken bij de voorbereidingen.

Draaiboeken

Besluitvorming over de draaiboeken vond plaats in het driehoeksoverleg. Uitgangspunt was dat alle maatregelen ertoe moesten leiden dat Koninginnedag 2009 op een veilige, ongehinderde, feestelijke en ordentelijke wijze zou verlopen. Tijdens de voorbereiding zijn diverse draaiboeken, vergunningen en plannen opgesteld. Meerdere processen en het command- and controlsystem zijn vooraf beoefend en op 29 april is een generale repetitie gehouden. Op 29 en 30 april zijn er briefings geweest waarin alle medewerkers op de hoogte zijn gesteld van de gang van zaken op Koninginnedag. De Inspectie OOV merkt op dat de verschillende organisaties de voorbereiding gedegen hebben opgepakt en dat er veel maatregelen in de voorbereiding zijn genomen.

Scenario's

De Inspectie OOV constateert dat de verschillende organisaties in hun draaiboeken verschillende scenario's voor Koninginnedag 2009 hebben gehanteerd en deze deels op een andere manier hebben uitgewerkt. Dit kon leiden tot verwarring bij de aanpak van incidenten en kon afstemmingsproblemen veroorzaken. Tijdens de incidentafhandeling heeft dit geen consequenties gehad omdat het toegepaste scenario 'Aanslag op het Koninklijke gezelschap' wel op uniforme wijze was uitgewerkt. De Inspectie vindt dat een multidisciplinaire aanpak een betere afstemming bij de uitwerking van de scenario's vereist.

Uitvoering evenement Koninginnedag 2009

Over het algemeen stelt de Inspectie vast dat de uitvoering van het evenement plaatsvond volgens de beslissingen die in de voorbereidingsfase zijn genomen. De Inspectie staat bij één uitvoeringsaspect in het

bijzonder stil, te weten de wijze waarop invulling is gegeven aan het zogenoemde 'hekkenplan'. Gaandeweg het onderzoek waren er namelijk veel vragen over de wijze waarop de hekken langs de route tijdens het incident feitelijk waren geplaatst.
De Inspectie OOV constateert dat de wijze waarop de hekken op Koninginnedag ter hoogte van de kruising Jachtlaan en Loolaan waren geplaatst, een logisch uitvloeisel was van de voorbereide activiteiten en genomen besluiten. Bij het plaatsen van de hekken is conform het verleende mandaat van de lokale driehoek gehandeld. De plaatsing van de hekken had als doel te voorkomen dat er zich publiek zou bevinden op de route van de Koninklijke stoet. Hoewel in de ochtend mensen uit het publiek zich zelfstandig in de U-corridor bevonden, en dus niet achter een hek stonden, bleef het publiek ter hoogte van de Jachtlaan door de vorming van een fysieke afscheiding door de ceremoniële afzetting en de verkeersregelaars buiten de route van de stoet.

Afhandeling van het incident

Na het incident zijn functionarissen van de verschillende hulpverleningsdiensten direct in actie gekomen. In eerste instantie richtten deze acties zich met name op medische hulpverlening aan slachtoffers, het in veiligheid brengen van de Koninklijke familie en het controleren of de locatie van het incident veilig was. Vervolgens werd nog een groot aantal activiteiten opgestart.

Informatie-uitwisseling en afstemming: GRIP-afkondiging en tweede CoPI

De Inspectie OOV stelt vast dat bij de incidentafhandeling de fase van GRIP 3 was afgekondigd. Deze keuze wijkt af van het in de voorbereiding beschreven scenario 'Aanslag op het Koninklijk gezelschap' dat uit ging van GRIP 4. Verder bleek dat de verschillende gremia van de rampenbestrijdingsorganisatie gedurende langere tijd tegelijkertijd verschillende GRIP-fasen hanteerden en dat deze zonder onderlinge afstemming waren afgekondigd. De afwijking van de in het scenario aangegeven GRIP-fase en het gebrek aan onderlinge afstemming hebben geen aantoonbare problemen veroorzaakt, maar hebben wel geleid tot 'ruis'.
Ook bleek dat binnen de hulpverleningsstructuur onduidelijkheid bestond over het 'slapend' CoPI. Nadat het incident had plaatsgevonden is een (tweede) CoPI ingericht dat niet bij iedereen bekend was, waarvan de functie niet voor alle betrokkenen duidelijk was en dat vrij snel weer werd opgeheven. Het onnodig bijeen laten komen van het CoPI kostte menskracht. Bovendien droeg de verwarring over het al dan niet bestaan en de functie van het tweede CoPI niet bij aan een efficiënte hulpverlening.

Verbindingen

De Inspectie OOV constateert verder dat er tijdens de afhandeling van het incident problemen met de verbindingen waren. Dit gold zowel voor C2000 als voor de mobiele telefonie. Het C2000 netwerk was de gehele dag operationeel maar vertoonde kort na het incident congestie in de spraakaanvragen. Niet alle hulpverleningsdiensten konden gebruik maken van telefoons met een priority-status. De Inspectie merkt op dat verbindingen een aandachtspunt blijven zoals ook is geconstateerd in haar rapport over de Poldercrash[1].

Overdracht opsporingsonderzoek van regiokorps NOG naar Dienst Nationale Recherche (DNR)

De Inspectie OOV constateert dat bij de overdracht van het strafrechtelijk onderzoek van de regiopolitie NOG naar de DNR meermalen onduidelijkheid ontstond over zowel de wijze als over het moment van de overdracht. Het huidige Opsporingsprotocol Contra-Terrorisme biedt onvoldoende houvast voor de concrete invulling van de overdracht van een opsporingszaak van de regiopolitie naar de DNR. Onduidelijkheid ten aanzien van moment en wijze van overdracht kan ten koste gaan van een effectieve opsporing. Het draagt niet bij aan een professionele uitvoering van het politiewerk.

Slachtofferidentificatie, -registratie en -informatie

De Inspectie OOV constateert dat een zorgvuldige identificatie van overleden slachtoffers mede door de aard van de verwondingen de nodige tijd heeft gekost. Daarnaast verliep de totstandkoming van een slachtofferlijst van niet overleden slachtoffers stroef. Dit kwam onder meer omdat er niet werd gewerkt met de (nationale) gewondenkaart die geldt als de landelijke professionele norm bij de GHOR en omdat ziekenhuizen niet direct gegevens wilden doorgeven aan de autoriteiten in verband met het medische beroepsgeheim van de arts en de zorgplicht van de ziekenhuizen. Het eerder uitgevoerde onderzoek door de Inspectie OOV naar de Poldercrash wijst uit dat de totstandkoming van een slachtofferlijst vaker een probleem is. Ook bij de afhandeling van dit incident is de gewondenkaart niet gebruikt. Voor de snelle informatievoorziening aan de familie over de verblijfplaats van de getroffenen is het noodzakelijk dat het Actiecentrum CRIB tijdig over de juiste informatie beschikt. De Inspectie vindt het noodzakelijk deze zo belangrijke informatie-uitwisseling gedegen te borgen.

[1] Rapport 'Poldercrash 25 februari 2009; een onderzoek door de Inspectie Openbare Orde en Veiligheid, in samenwerking met de Inspectie voor de Gezondheidszorg', van 17 juni 2009.

Kabinet wil niet dat Koninginnedag wezenlijk verandert

Het kabinet wil niet dat het open en feestelijke karakter van Koninginnedag wezenlijk verandert. Het kabinet beseft dat nooit alle risico's zijn uit te sluiten en zal zich blijven inzetten voor een evenwicht tussen feestelijkheid en veiligheid tijdens nationale evenementen. Dat schrijven de ministers van Justitie en BZK in de kabinetsreactie op de onderzoeksresultaten naar de gebeurtenissen op Koninginnedag.

Het maatregelenpakket voor de beveiliging van Koninginnedag 2009 was omvangrijk en grondig voorbereid. De voorbereide maatregelen zijn vrijwel geheel zoals beoogd uitgevoerd. Desondanks is met dit pakket van beveiligingsmaatregelen een aanslag als deze niet voorkomen. De ministers vinden dat de verantwoordelijkheden en bevoegdheden in het stelsel afdoende zijn geregeld om adequate besluitvorming mogelijk te maken. Het stelsel is echter niet op alle onderdelen voldoende uitgewerkt. Wanneer rijks- en decentrale verantwoordelijkheden rond bewaken en beveiligen samenkomen, zoals bij Koninginnedag, geeft de NCTb tot dusverre alleen advies richting lokaal bevoegd gezag in geval van verhoogde dreiging of risico. Samenhang van het geheel van beveiligingsmaatregelen is daardoor niet in alle gevallen gewaarborgd. In de toekomst moet de structurele regie ten behoeve van samenhang en afstemming tussen partijen in het proces van bewaken en beveiligen rond nationale evenementen als Koninginnedag worden versterkt.

Daarnaast zijn verbeteringen mogelijk in de uitvoering van het stelsel en in het proces van het bepalen van het dreigingsniveau; de afwegingen die worden gemaakt tussen beveiliging en andere belangen; en de wijze waarop de beveiligingsfunctie van diverse maatregelen (zoals beveiligingsringen) expliciet wordt gemaakt.

Naar aanleiding van het Inspectierapport heeft de minister van BZK het Veiligheidsberaad verzocht om met alle C2000-gebruikers na te gaan of deze procedures voldoende helder zijn uitgewerkt en bij alle hulpverleners bekend en geoefend zijn. In samenhang daarmee zal de minister van BZK – indien daar aanleiding toe is – nagaan in hoeverre het mogelijk is om de capaciteit van het C2000-netwerk binnen de beschikbare frequentieruimte te optimaliseren.

Met betrekking tot de uitwisseling van slachtofferinformatie zal het kabinet bij het Veiligheidsberaad, de Vereniging voor Nederlandse Gemeenten (VNG), Ambulancezorg Nederland en de Nederlandse Vereniging van Ziekenhuizen aandacht vragen voor deze problematiek en aandringen op heldere afspraken tussen betrokken partijen in een landelijk geldend protocol.

Bij evenementen van nationaal belang, die worden bezocht door personen die vermeld staan op de zogeheten limitatieve lijst én waarbij het karakter van het evenement een specifieke of verhoogde druk op de beveiliging kan leggen, zal de NCTb voortaan altijd advies geven over samenhang van beveiligingsmaatregelen en de afstemming tussen betrokken partijen, ongeacht het dreigings- of risiconiveau.

In de toekomst zal de NCTb met alle betrokken partijen tot de vaststelling van landelijke afgestemde dreigingsscenario's komen en deze periodiek actualiseren. Deze dreigingsscenario's moeten bijdragen aan een meer systematische afweging bij het vertalen van voorstelbare dreigingen in adequate beveiligingsmaatregelen. Ook zal in de toekomst bij evenementen van nationaal belang de systematiek van beveiligingsringen structureel gehanteerd worden.

Het kabinet benadrukt dat de werking van het stelsel van bewaken en beveiligen nooit alle risico's kan uitsluiten. Het kabinet is het erover eens dat dit streven zou leiden tot draconische beveiligingsmaatregelen die voorbij gaan aan de essentie; namelijk het veilig maar ook zo ongestoord mogelijk kunnen functioneren van te beveiligen personen. Bij de voorbereiding van de beveiliging kan echter blijken dat alternatieve beveiligingsmaatregelen noodzakelijk of gewenst zijn. In dat geval zullen deze wijzigingen worden opgenomen in de plannen die ter goedkeuring aan het bevoegd gezag, i.c. de lokale driehoek voor lokale domein en de NCTb voor het rijksdomein, worden voorgelegd.

(Bron: persbericht ministeries van BZK en Justitie, 4 september 2009)

Geert Wismans,
programma Nationale Crisisbeheersing op Orde
directie Nationale Veiligheid, ministerie van BZK

Ministerraad stelt nieuw Nationaal Handboek Crisisbesluitvorming vast

Eind november heeft minister Ter Horst namens het Kabinet een actuele versie van het *Nationaal Handboek Crisisbesluitvorming* aan de Tweede Kamer aangeboden. Het Handboek legt procedures en eenduidige coördinatie- en besluitvormingsstructuren op rijksniveau vast voor de beheersing van (dreigende) crises. Dit Handboek vervangt de sterk verouderde versie uit 2002. Het Handboek is herzien op basis van de verantwoordelijkheids- en rolverdeling conform het Beleidsplan Crisisbeheersing 2004-2007 (TK 2003-2004, 29 668, nr. 1) en het instellingsbesluit van de Ministeriële Commissie Crisisbeheersing, dat per 26 juli 2009 in werking is getreden (Staatscourant 24 juli 2009).[1]

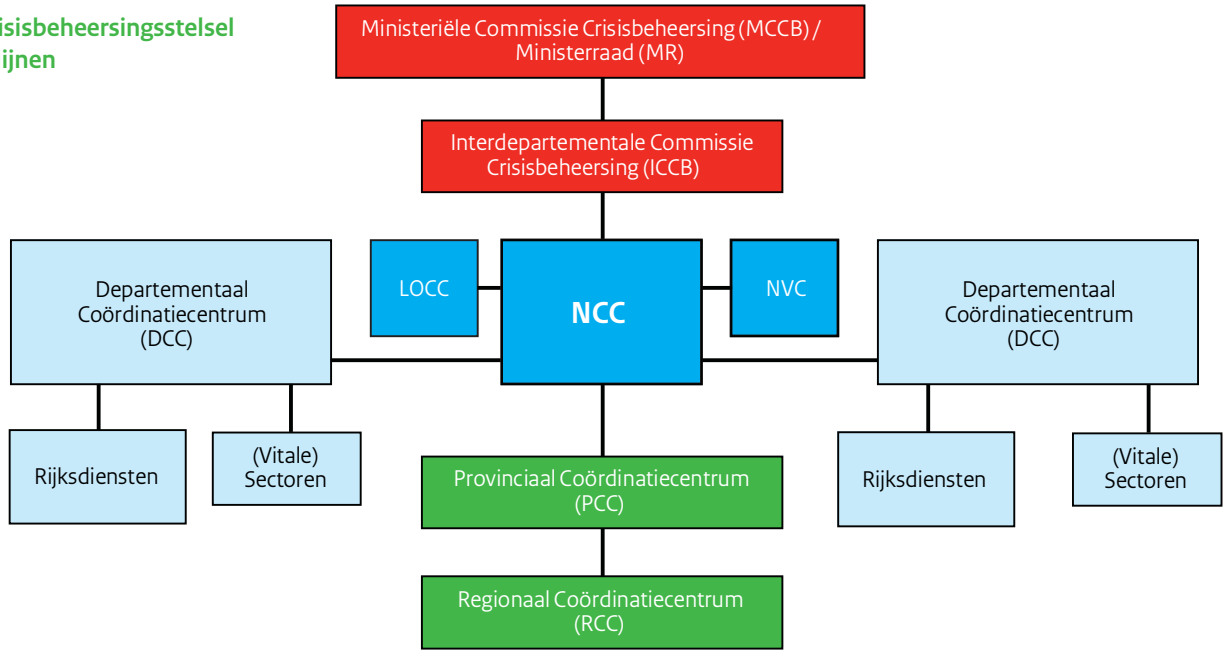
Crisisbesluitvorming op politiek-bestuurlijk niveau vindt plaats in de Ministeriële Commissie Crisisbeheersing (MCCB). De Interdepartementale Commissie Crisisbeheersing (ICCB) fungeert als voorportaal op hoog ambtelijk niveau. Het Nationaal CrisisCentrum (NCC) is de ondersteunende c.q. uitvoerende staf en het facilitair bedrijf ten dienste van de (voorbereiding van de) interdepartementale crisisbesluitvorming.

Het Handboek is per definitie een levend document dat periodiek wordt geactualiseerd naar aanleiding van lessen uit daadwerkelijke crises, evaluaties van oefeningen of wijzigingen in wet- en regelgeving.

Aanpassingen op basis van onder meer de aanstaande inwerkingtreding van de Wet veiligheidsregio's en de uitwerking van de nauwere samenwerking tussen de verschillende departementale coördinatiecentra (DCC's) en het NCC zullen worden meegenomen in een volgende versie van het Handboek die zomer 2010 verschijnt.

Het Handboek wordt aangeboden aan alle ministeries, bestuurders, voorzitters veiligheidsregio's en betrokken koepels met de aanbeveling om de herziene afspraken te implementeren in de plannen binnen hun eigen crisisorganisatie.

Figuur: Crisisbeheersingsstelsel op hoofdlijnen



[1] Zie Magazine nationale veiligheid en crisisbeheersing augustus/september 2009, 51.

Onder de titel 'Werk in uitvoering' organiseerde het ministerie van BZK op 10 november voor de zesde keer het jaarlijkse Veiligheidscongres. Het programma had dit jaar een internationale focus, dankzij bijdragen van Jan van Laarhoven, secretaris-generaal van de Benelux en Ken Livingstone, voormalig burgemeester van Londen. De twee keynote-speakers belichtten veiligheids-vraagstukken van internationaal belang, waarbij samenwerking over de grenzen heen cruciaal is.

Internationale focus
bij Veiligheidscongres 2009

Rob Jastrzebski

Benelux pionier veiligheid binnen Europa

In die grensoverschrijdende samenwerking lopen de Benelux-landen binnen Europa voorop. De Benelux is veel meer dan een economische unie. Veiligheid is al decennialang een van de speerpunten en binnen Europa vervult de Benelux zelfs een pioniersrol op dit gebied, stelt Van Laarhoven. Een hele reeks verdragen en samenwerkingsregelingen heeft geleid tot verbetering in de grensoverschrijdende politiesamenwerking, gezamenlijke aanpak van criminaliteit, samenwerking bij opsporing en vervolging én effectievere samenwerking op het gebied van crisisbeheersing en rampenbestrijding. Niet alleen op papier, maar ook in de praktijk.
Een belangrijke stap in de verbetering van de samen-werking op veiligheidsgebied in de grensstreken was de ondertekening in 1986 van een Benelux overeenkomst.

De praktijk van grensoverschrijdende politiesamen-werking kreeg onder meer gestalte in de gezamenlijke voorbereiding op het Europees Kampioenschap Voetbal door Nederland en België in 2000. Het bilaterale verdrag beperkte zich echter tot de duur van Euro 2000.
De evaluatie leidde tot de conclusie dat het succes van de samenwerking rond Euro 2000 een meer permanent vervolg moest krijgen. Dat gebeurde in 2004 met de ondertekening van het Verdrag van Senningen door de drie Beneluxlanden.

Het verdrag geeft politiediensten van de drie betrokken landen meer bevoegdheden voor grensoverschrijdend optreden, in spoedeisende gevallen, zelfs zonder toestemming vooraf.
Van Laarhoven benadrukte dat de afspraken niet blijven steken in goede intenties, maar regelmatig in de praktijk worden gebracht: "Een recent voorbeeld is de manifestatie van melkveehouders in Luxemburg op 18 oktober, waarbij de Belgische politie specialistische bijstand verleende. Bij de voetbalwedstrijd tussen AZ en Standard Luik kort geleden zorgden de Mobiele Eenheid uit België en Nederland gezamenlijk met succes voor handhaving van de openbare orde."
Inmiddels is het Verdrag van Senningen na vijf jaar toe aan een grondige evaluatie. Nederland, België en Luxemburg hebben toegezegd om vóór het eind van dit jaar een evaluatie op te stellen, met daaraan gekoppeld een behoefteanalyse en een lijst verbeterpunten om de grensoverschrijdende samenwerking verder te intensiveren en te verbeteren. Ondertussen is in juni 2008 voor de samenwerking in brede zin een nieuw verdrag ondertekend.

Londense lessen voor terreuraanpak

De stijd tegen radicalisering en terrorisme is één van de grote gemeenschappelijke veiligheidsvraagstukken in Europa. Een actuele en significante dreiging, met de

aanslagen in Madrid in 2004 en in Londen in 2005 als meest recent bewijs van de kwetsbaarheid van de westerse wereld. Ken Livingstone, voormalig burgemeester van Londen erkende die kwetsbaarheid na de aanslagen in New York in september 2001. Hij nam de congresbezoekers mee naar de overheidsbrede preparatie op aanslagen na de schok van 11 september en maakte duidelijk hoe de vruchten van die inspanningen konden worden geplukt, toen Londen in juli 2005 zelf het doelwit was.

Een cruciale stap was volgens Livingstone het instellen van een 'resilience committee', waarin alle overheidsinstanties met een taak op veiligheidsgebied waren vertegenwoordigd. Het comité moest de veerkracht van de metropool versterken en kaders opstellen voor het overheidsoptreden in geval van een terroristische aanslag. De dag na 11 september toog het comité aan de slag, met het opstellen van een risico-analyse, het identificeren van mogelijke doelwitten voor aanslagen en het maken van stringente afspraken over bevoegdheden en verantwoordelijkheden; zelfs voor worst case-situaties waarin de verantwoordelijken op het hoogste niveau als gevolg van een aanslag zouden zijn uitgeschakeld. Heldere mandaten voor alle beslissingsniveaus werden vooraf geregeld.
Livingstone zag in dat de strijd tegen extremisme en preventie van terroristische aanslagen een zaak van lange adem zou worden. Een sterk publiek vertrouwen in het openbare orde en veiligheidsapparaat zag hij daarbij als belangrijkste voorwaarde voor succes. "Om te beginnen moest het hoofdstedelijk politieapparaat worden versterkt. De slagkracht van het korps was in de loop der jaren verminderd, terwijl de burgers voor hun veiligheidsgevoel juist baat hebben bij een sterk zichtbare aanwezigheid van de politie in het straatbeeld."
Volgens Livingstone moesten de autoriteiten in Londen op 12 september van voren af aan beginnen met strategische planvorming tegen terreuraanslagen. Hoewel de Engelse hoofdstad in het verleden wel met de nodige aanslagen van de IRA te maken had gehad, was de dreiging die na 11 september 2001 ontstond van een geheel andere orde.
Livingstone: "Het Noordierse vraagstuk werd opgelost door dialoog op het politieke vlak, zodat de directe dreiging van aanslagen uit die hoek sterk was verminderd. De urgentie voor een krachtige preparatie op terreuraanslagen was tot 11 september 2001 niet aanwezig. Dat veranderde op slag. De grote schok van de aanslagen in New York was dat extremisten in westerse hoofdsteden aanslagen konden plegen op een schaal die daarvoor nauwelijks voorstelbaar was. De tweede schok was dat zij hun plannen ten uitvoer konden brengen zonder dat inlichtingendiensten hiervoor concrete aanwijzingen hadden. De aanslagen in New York en Washington waren in dat opzicht een eye-opener. En wij realiseerden ons dat Londen heel goed tweede op de lijst favoriete locaties zou kunnen zijn voor terroristen op zoek naar een geschikt doelwit."
De aanslagen op de Londense metro en een autobus in juli 2005 konden ondanks de brede Londense aanpak niet worden voorkomen, maar toch heeft de stad volgens Livingstone in meerdere opzichten geluk gehad. De krachtige aanpak na september 2001 had tot gevolg dat de overheid op het Uur U als een geoliede machine in actie kwam en dat de verdeling van taken, bevoegdheden en verantwoordelijkheden bij politie, justitie, de hulpverlening en het gemeentebestuur volstrekt helder was. Livingstone prijst ook de veerkracht van de bevolking en is er trots op dat de multiculturele hoofdstad na de aanslagen niet te maken kreeg met conflicten en gewelddaden tussen bevolkingsgroepen onderling.
Livingstone: "Een aanslag komt natuurlijk nooit gelegen, maar ik ben blij dat we na 11 september 2001 vier jaar de tijd hebben gehad om ons voor te bereiden en dat we niet al vier maanden later zelf door een aanslag waren getroffen. Dan was ons optreden een groot fiasco geworden, omdat we er op dat moment beslist niet klaar voor waren. Vier jaar grondige voorbereiding door alle overheidsdiensten kon in juli 2005 worden vertaald in daadkracht en veerkracht."

Grote belangstelling voor de interactieve, multimediale workshop NCC

Workshops

In de middag vonden er diverse workshops plaats op het terrein van nationale veiligheid en crisisbeheersing, zoals een multimediale workshop over de werkwijze van het Nationaal Crisiscentrum, werken met bestuurlijke netwerkkaarten crisisbeheersing, bestuurders aan de slag na een ramp en crisisbeheersing in 2029.

Hulpverleners moeten op C2000 kunnen vertrouwen

Leo Nieuwenhuizen,
programmamanager Veiligheid, Informatie en Technologie, DG Veiligheid, ministerie van BZK

Dit jaar zijn er drie grootschalige incidenten geweest, te weten de vliegtuigramp met een toestel van Turkish Airlines (Poldercrash), de aanslag in Apeldoorn op Koninginnedag en de ongeregeldheden op het strand van Hoek van Holland. In al deze gevallen zijn hulpverleners geconfronteerd met communicatieproblemen tijdens de afhandeling van de incidenten.

Uit de verkeersgegevens van het C2000-netwerk blijkt dat in het geval van de Poldercrash en bij Apeldoorn er sprake is geweest van overbelasting van C2000 masten rond het crisisgebied. Hoewel C2000 volledig operationeel was, kwamen niet alle spraakaanvragen gelijk tot stand. Zo onderhielden tijdens de vliegtuigcrash ambulances die uit andere regio's kwamen om bijstand te verlenen, ook nog via C2000 contact met hun thuisregio. Dat was volgens de huidige regels, maar belastte onnodig de dichtstbijzijnde C2000-mast in de buurt van Schiphol.

Binnen C2000 wordt gewerkt met gespreksgroepen om de communicatie tussen hulpverleners te ordenen. Het gebruik van veel verschillende gespreksgroepen vraagt veel capaciteit, waardoor overbelasting kan ontstaan. Het gebruik van weinig gespreksgroepen met veel gebruikers leidt niet tot overbelasting. Doordat maar één gebruiker binnen een gesprekgroep tegelijk kan communiceren, ontstaat voor andere gebruikers de indruk dat overbelasting is opgetreden. Bij alle drie de incidenten heeft deze situatie zich voorgedaan.

Minister Ter Horst heeft aangegeven dat zij het van groot belang vindt, dat de communicatieproblemen snel worden opgelost. Het vertrouwen in het systeem onder de hulpverleners is de afgelopen periode afgenomen. Zij heeft daarom een expertgroep in het leven geroepen die onderzoek doet naar de oorzaken van de problemen met C2000. De expertgroep bestaat uit operationele leidinggevenden uit de diverse sectoren en de leverancier van C2000.

De experts kijken zowel naar de techniek (capaciteit van masten en netwerk) als naar de regels voor het gebruik van C2000 (wordt er wel een goede etherdiscipline nageleefd) door de hulpverleningsdiensten als naar de organisatorische aspecten (zijn de procedures voor het gebruik van C2000 tijdens grootschalige incidenten wel compleet, bekend en geoefend bij de gebruikers).

De groep experts zal ook kijken naar de uitkomsten van het onderzoek naar de problemen die enkele brandweerkorpsen hebben met het gebruik van portofoons in gebouwen, buiten het C2000-netwerk om, direct van portofoon naar portofoon. Een paar

Met C2000 is één multidisciplinair landelijk communicatiesysteem ontwikkeld voor de hulpverleningsdiensten. Dit digitale netwerk verving bijna honderd afzonderlijke analoge netwerken in Nederland. C2000 is al eens bestempeld als een van de grootste samenwerkingsverbanden binnen de overheid. Zeshonderd partijen op alle overheidsniveaus, elk met hun eigen werkwijzen, cultuur, doelstellingen werkten samen om te komen tot één landelijk multidisciplinair en digitaal communicatienetwerk .

brandweerkorpsen gebruiken in dat soort omstandigheden weer analoge portofoons, in plaats van digitale C2000-portofoons.

Inmiddels heeft de expertgroep haar eerste tussenrapportage uitgebracht. Volgens de groep experts moeten de afspraken volledig herschreven worden naar een nieuw multidisciplinair document, met procedures over bovenregionale, landelijke en interregionale bijstand tussen de verschillende diensten, toegesneden op crisissituaties. Ook over de opleidingen aan de operationele gebruikers, het meldkamerpersoneel en de regionale beheerders moeten volgens de experts betere afspraken worden gemaakt, net als over oefeningen.

Daarnaast doet de expertgroep in haar tussenrapportage aanbevelingen over het wegwerken van de zogenoemde DIPP lijst (Dekkings Issue Prioritering Procedure) en het starten van het overleg via het Agentschap Telecom met het ministerie van Defensie over het beschikbaar stellen van additionele frequenties. De capaciteit van het C2000 netwerk kan worden uitgebreid door extra radiofrequenties in te zetten die bij Defensie zijn vrijgekomen.

In reactie op deze tussenrapportage wil minister Ter Horst de resterende 60 locaties in Nederland met verminderde dekking binnen twee jaar wegwerken, in plaats van binnen acht jaar. Dat gebeurt door versneld C2000-masten bij te bouwen of door technische veranderingen aan bestaande masten aan te brengen. Verder wil de minister met extra radiofrequenties de capaciteit van C2000 vergroten. Ter Horst wil het systeem zo verbeteren dat de hulpverleners erop kunnen vertrouwen dat C2000 goed werkt en daarmee bereiken dat zij (weer) vertrouwen in C2000 hebben.

Het zou technisch mogelijk zijn om capaciteit binnen het C2000-netwerk te verplaatsen, bijvoorbeeld van Zeeland en het noorden en oosten van het land naar de Randstad. Dit is echter een complexe operatie en bovendien is het de vraag of een dergelijke verplaatsing geaccepteerd zou worden in regio's die erop achteruit gaan. Daar kunnen zich immers ook calamiteiten voordoen. De oplossing wordt daarom liever gezocht in het uitbreiden van de capaciteit. Hiervoor zijn wel extra radiofrequenties noodzakelijk. Er zal gekeken worden of de uitbreiding van de freguentieruimte mogelijk is, hiervoor zal het ministerie van Economische Zaken benaderd worden.

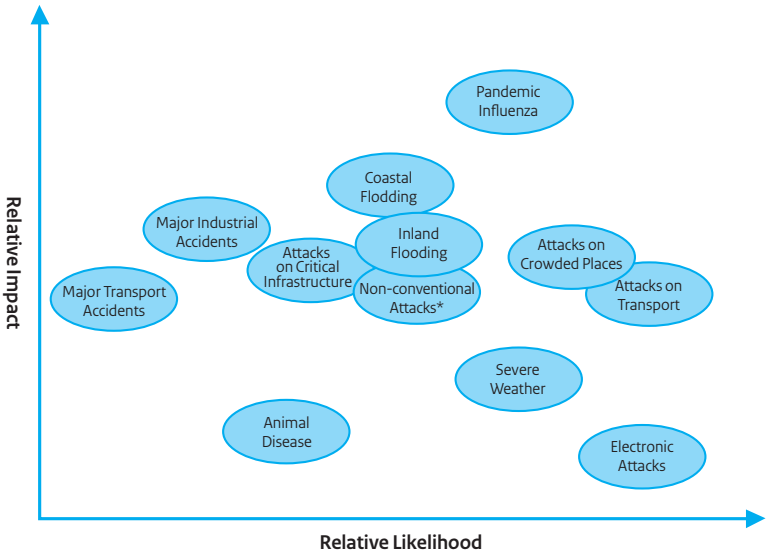
Ter Horst heeft het Veiligheidsberaad gevraagd de landelijk vastgestelde indeling in gespreksgroepen en operationele procedures te saneren en aan te vullen, ook met het oog op grote calamiteiten. De groep experts komt voor het einde van het jaar met een eindrapportage. In januari volgend jaar volgt er een Kabinetsstantpunt over de eindrapportage van de expertgroep.

Crisis Computing:
beslissingsondersteuning in een complexe wereld

prof. dr. Peter M.A. Sloot,
directeur Instituut voor Informatica,
Universiteit van Amsterdam

We leven in een complexe wereld waar we overladen worden met informatie en voortdurend beslissingen moeten nemen, rekening houdend met 1001 verschillende bronnen van informatie. Dit is niet enkel het geval in het dagelijkse leven, maar geldt zeker ook voor de manier waarop we over de veiligheid in ons land moeten waken en beslissingen moeten nemen in geval van een acute crisis.

Informatie uit apparatuur, observaties, databases, literatuur, experimenten etc. moeten we verzamelen, analyseren, combineren en begrijpbaar maken. De informatiebronnen zijn vaak verspreid over vele locaties en van totaal verschillende aard: Een database uit de Verenigde Staten, een sensor in een dijk, een weersvoorspelling simulatie, een stuk tekst in een krant of op een weblog, een video van een bewakingscamera, allemaal bronnen van veelsoortige informatie waaruit we moeten putten om complexe beslissingen te ondersteunen.



Figuur 1: De kans op een nationale ramp uitgezet tegen de mogelijke gevolgen van zo een ramp.
(bron: National Risk Register, Cabinet Office, UK).

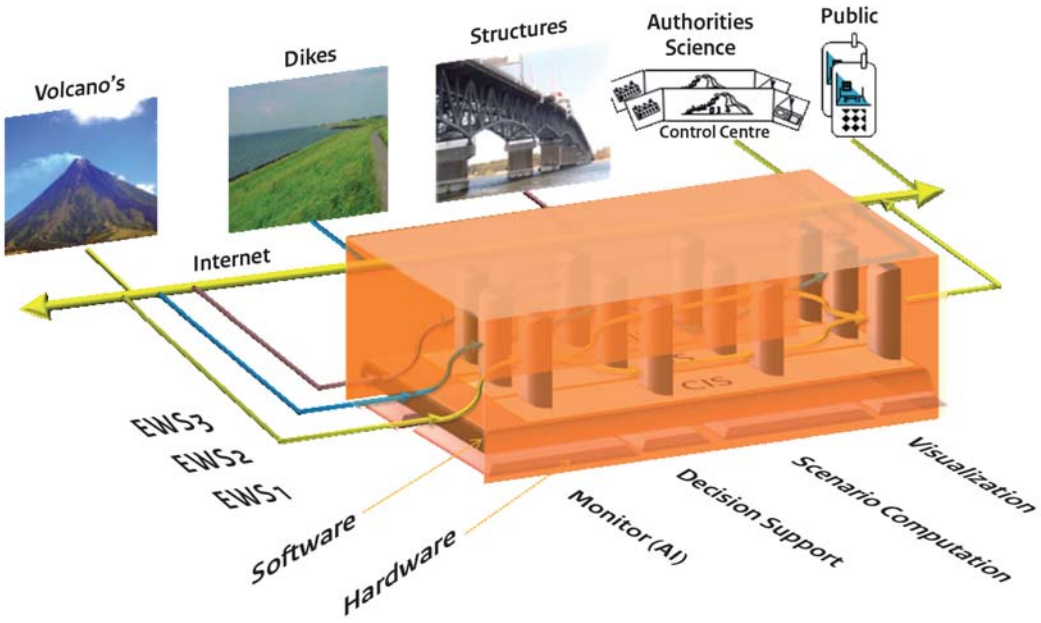
Recent onderzoek in het Verenigd Koninkrijk brengt de *kans* op een calamiteit tegen de mogelijke *impact* daarvan in kaart (figuur 1).

Vergelijkbaar onderzoek in Nederland is eerder gepubliceerd in dit tijdschrift[1]. Nadere analyse van deze mogelijke nationale rampen laat duidelijk zien dat het snel verkrijgen van informatie samen met het snel doorrekenen van mogelijke ramp scenario's en scenario's voor de crisisbeheersing essentieel zijn. Neem bijvoorbeeld de manier waarop we in de toekomst beslissingen zullen moeten nemen bij een dreigende pandemie uitgaande van informatie uit allerlei bronnen zowel over de interactie tussen individuele mensen als kennis over het virus. Hierbij dienen we virale moleculaire informatie te koppelen aan ondermeer sociale contact netwerk informatie[2], ten einde een goed onderbouwde beslissing voor de beheersing van de pandemie te kunnen nemen. Of neem de gevolgen van

[1] *Magazine nationale veiligheid en crisisbeheersing* 7 nr. 6 (juni/juli 2009), 18 ev.

[2] P.M.A. Sloot, P.V. Coveney, G. Ertaylan, V. Müller, C.A.B. Boucher and M.T. Bubak, 'HIV Decision Support: From Molecule to Man', in: *Philosophical Transactions of the Royal Society A*, vol. 367, nr 1898 (2009), 2691-2703. (DOI: 10.1098/rsta.2009.0043)

Figuur 2: Software architectuur van het 'UrbanFlood' project, waarbij sensorische informatie gevoed wordt in computer simulaties en scenario's kunnen worden doorgerekend.



klimaatverandering op onze dijken. Grote delen van Nederland bestaan bij gratie van onze dijken. Dreigingen door veranderingen in de hoeveelheid water dat ons land binnen stroomt via de grote rivieren en verandering in de zeespiegel kunnen vragen om acute en complexe beslissingen. Hierbij dient geografische informatie gekoppeld te worden aan weers- en klimaat-modellen en aan informatie over sluisstanden, bezettingsgraad van uiterwaarden, fysische modellen voor dijk stabiliteit etc.

Het goede nieuws is dat we inderdaad veel meer informatie kunnen genereren. Het slechte nieuws is dat we zelden een idee hebben hoe die verschillende bronnen van informatie met totaal verschillende ruimte- en tijdschalen te combineren, toegankelijk te maken en zowel kennis als betrouwbare beslissingen eruit te destilleren.

Wat nodig is, is een integrale, holistische, aanpak waarbij we een geavanceerde en veilige ICT infrastructuur aanleggen om de data uit al die verschillende bronnen te integreren. Dat is echter pas het begin, echt lastig wordt het zodra we scenario's door middel van computer simulaties willen doorrekenen zodat we de rampen kunnen voorspellen en de parameters welke de invloed van de ramp bepalen kunnen beoordelen. Hiertoe moet niet alleen snel verschillende supercomputers kunnen worden ingeschakeld, maar ook geheel nieuwe computationele methoden ontwikkeld worden, immers hoe kunnen we informatie welke zich uitstrekt over zoveel dimensies en disciplines zinvol combineren tot een beslissingsadvies voor de beleidmakers en crisismanagers?

Binnen het Instituut voor Informatica van de Universiteit van Amsterdam wordt samen met een groot aantal andere instituten en bedrijven gewerkt aan innovatieve computationele methoden voor gedistribueerde beslissingsondersteuning. Zo wordt al jaren gewerkt aan een nieuw systeem om infectieziekten, hun verspreiding en behandeling te modelleren binnen het *virolab* project[3].

Een ander voorbeeld is het recent gehonoreerde Europese project gehonoreerd met de naam 'UrbanFlood'. Hierbij worden dijken en andere erosie gevoelige structuren door middel van sensor netwerken voortdurend in de gaten gehouden en wordt de sensor informatie gekoppeld aan ondermeer satelliet data en weersvoorspelling data. In dit project wordt intelligente software ontwikkeld welke indien nodig zelfstandig extra supercomputers kan inschakelen en specifieke netwerk bandbreedte kan afdwingen (zie figuur 2). Nieuwe computationele modellen rekenen dan scenario's door waarmee snel en adequaat beslissings-voorstellen kunnen worden afgeleid voor crisismanagers.

'Crisis computing' zal in de nabije toekomst een grote rol gaan spelen op vele plaatsten waar snel en efficiënt beslissingsondersteuning nodig is in een steeds complexer wordende samenleving. De eerste stappen worden wereldwijd gezet, we staan nog maar aan het begin, er is nog veel onderzoek nodig en de tijd dringt.

[3] www.virolab.org.

Méér rendement

uit opleiden, trainen en oefenen in voorbereiding op crises

drs. C. Timmer en drs. N. Schuurhuizen,
Beiden werkzaam als psycholoog-trainer bij Trimension BV

Opleidingen, trainingen en oefeningen (OTO) zijn essentiële onderdelen van de voorbereiding op crisis. Hoewel in OTO veel energie en geld wordt geïnvesteerd, is de hoeveelheid tijd die functionarissen er per jaar aan kunnen besteden veelal aan duidelijke grenzen gebonden. Trainers en docenten zoeken daarom continu naar mogelijkheden om de beschikbare tijd zo goed mogelijk te benutten en om zo veel mogelijk resultaat binnen die tijd te behalen. Dit artikel geeft een aantal suggesties waarmee het mogelijk is om zonder extra investeringen het rendement van OTO te verbeteren. De auteurs baseren zich op praktijkervaringen gekoppeld aan inzichten uit de (organisatie)psychologie.

Liever vaker korte en afwisselende modules dan één lange

De realiteit leert ons dat er jaarlijks relatief weinig tijd per deelnemer beschikbaar is om te besteden aan opleidingen, trainingen en oefeningen in de voorbereiding op crisis. De tijd die er is wordt veelal geconcentreerd ingezet door gedurende één dag op te leiden, te trainen of te oefenen. Van Ebbinghaus[1], pionier in het geheugenonderzoek, weten we echter dat het grootste deel van nieuw geleerde informatie zonder herhaling vergeten wordt binnen een uur na het leren. Daarbij komt dat volwassenen een aandachtsspanne van ongeveer 20 minuten hebben, waardoor langdurige informatieoverdracht weinig leerrendement oplevert. Door informatie op de juiste momenten kort te herhalen over een langere periode is het mogelijk vrijwel 100% van de informatie te onthouden. Toegepast op crisisbeheersing is het dus van belang tijdens OTO meerdere korte opleidingsmomenten in te lassen waarbij overdracht van tot de kern teruggebrachte informatie wordt afgewisseld met korte toegepaste oefeningen en herhaling.

Benut competenties en middelen óók in dagelijkse praktijk

Tot nu toe worden de tijdens OTO opgedane competenties en aangeschafte middelen nog vaak beperkt ingezet in de dagelijkse praktijk. Hierdoor is

[1] D. Groome e.a., *An Introduction to Cognitive Psychology; Processes and Disorders*, Hove, Psychology Press, 2006.

het voor deelnemers extra moeilijk om de tijdens OTO opgedane kennis en vaardigheden te gebruiken tijdens daadwerkelijke crises omdat die in de regel niet zo vaak voorkomen. Een eenvoudig voorbeeld hierbij zijn smartboards die zijn aangeschaft om tijdens crisis informatie te kunnen delen. In de dagelijkse praktijk worden deze vaak niet of nauwelijks gebruikt, waardoor de opgedane vaardigheden om hiermee om te gaan langzaam wegebben. Wanneer zich een crisis voordoet, kost het dan veel tijd om het werken met de smartboards soepel te laten verlopen. De Galan[2] noemde in één van haar trainersbestsellers al dat wanneer deelnemers niet meteen in de praktijk toepassen wat ze hebben geleerd, slechts ongeveer 5% van het geleerde onthouden wordt. Echter, wanneer deelnemers het geleerde regelmatig in de praktijk toepassen, wordt 90% van de opgedane competenties behouden. Door competenties en middelen die men tijdens crises nodig heeft regelmatig toe te passen in de dagelijkse praktijk – en daarmee te herhalen – vergroot men het rendement van OTO en versterkt men de crisisorganisatie. Daarnaast verbetert het de kwaliteit van de dagelijkse werkzaamheden. Smartboards hebben namelijk genoeg functies die men ook tijdens dagelijkse vergaderingen goed kan gebruiken. Dit geldt eveneens voor bijvoorbeeld de crisisvergader-agenda, scenarioanalyse, netwerkanalyse etc.

Investeer in vergroten self-efficacy bij deelnemers en crisisteams

Om tijdens crises adequaat en efficiënt te kunnen handelen is het opdoen van competenties alleen niet voldoende. De reële overtuiging van deelnemers dat ze adequaat en efficiënt kunnen handelen en daarmee bepaalde doelen kunnen bereiken, is wellicht nog veel belangrijker. Bandura[3] gaf aan dit fenomeen de naam self-efficacy en verrichte hier veel onderzoek naar. Hij concludeerde dat het beschikken over reële *self-efficacy* essentieel is voor het hebben van controle, overzicht, motivatie en succes bij veeleisende taken. De twee belangrijkste factoren die self-efficacy bevorderen zijn het zelf ervaren van succes en het zien van succes bij gelijkgestemden. Voor het presteren tijdens crises is het van belang om deelnemers al in de preparatiefase successen te laten ervaren. Allereerst zal dit individueel moeten gebeuren door middel van interactieve opleidingen waarbij aandacht is voor de competenties en behoeften van deelnemers. Vervolgens kunnen de groepsleden in trainingen en oefeningen gaan leren van en met elkaar, waarbij de trainer een meer coachende en faciliterende rol op zich neemt en de groep zelf succeservaringen creëert. De groepsleden krijgen op deze manier meer self-efficacy en leren hoe ze van elkaar kunnen leren, om als crisisteam adequater te functioneren en zich te blijven verbeteren. Dit is extra relevant, omdat het tijdens crises niet vanzelfsprekend is dat alles meteen goed gaat. Self-efficacy betekent dat men moet vertrouwen op het zelflerend vermogen waarmee men in staat is om tijdens crises gecoördineerd te improviseren.

Deelnemers motiveren

De tot nu toe besproken suggesties voor het verbeteren van het rendement van OTO hebben allemaal nog een extra toegevoegde waarde: ze zorgen voor meer motivatie bij deelnemers. De gedachte dat deelnemers één keer per jaar opgeleid, getraind of beoefend worden voor iets wat waarschijnlijk nooit gebeurt, is niet motiverend. Wanneer het OTO-traject interactief ingedeeld wordt met meerdere korte en afwisselende opleidingen, trainingen en oefeningen, klinkt dit al aantrekkelijker. Door de tijdens OTO geleerde lessen toepasbaar te maken in de dagelijkse praktijk, ontstaat ook extra toegevoegde waarde voor de organisatie. Voeg daar het vergroten van de reële self-efficacy aan toe en een opleiding, training of oefening draagt ook nog eens bij aan het persoonlijk functioneren van de deelnemers. Uit diverse wetenschappelijke onderzoeken[4] blijkt dat variatie, samenwerking, blijven leren van elkaar en self-efficacy, leiden tot meer motivatie. Gemotiveerde personen zijn bereid om meer inspanningen te leveren. Kortom: de in dit artikel gedane suggesties dragen bij aan de motivatie, inzet en betrokkenheid van deelnemers tijdens de voorbereiding op en daadwerkelijke uitvoering van (crisis) werkzaamheden.

Resumé

In onze dagelijkse praktijk hebben we gemerkt dat het doorvoeren van de in dit artikel gedane suggesties ertoe leidt dat deelnemers ervaren dat crisispreparatie ook leuk kan zijn en dat de geleerde lessen veel breder toepasbaar zijn dan voorheen het geval was. Door het opvolgen van deze suggesties neemt het rendement van de inspanningen op het gebied van OTO toe, iets dat extra relevant zal zijn onder de huidige economische omstandigheden. Tegelijkertijd ontstaat vanuit de grotere motivatie en betrokkenheid van de deelnemers beter zicht op hun specifieke behoeften waardoor een opleidingscoördinator de benodigde investeringen kan onderbouwen om de crisispreparatie naar een hoger niveau te tillen.

[2] K. de Galan, *Trainingen ontwerpen*, Amsterdam: Person Education Benelux, 2007.

[3] A. Bandura, *Self-Efficacy. The Exercise of Control*, New York: W.H. Freeman & Company, 1997.

[4] J.J. Boonstra e.a., *Dynamics of Organizational Change and Learning*, Chichester, England: John Wiley & Sons Ltd, 2007.

Fatma Aytekin,
Nationaal CrisisCentrum

Het Nationaal CrisisCentrum (NCC) heeft op 25, 28 en 29 september 2009 deelgenomen aan de EU oefening CCAEX09 (Emergency and Crisis Coordination Arrangements).
In samenwerking met het ministerie van Buitenlandse Zaken en de NCTb heeft het NCC vanuit een responscel Nederlandse input geleverd richting de Permanente Vertegenwoordiging van Nederland bij de Europese Unie in Brussel. CCAEX is een jaarlijkse EU-oefening in Brussel waarbij tot en met de ambassadeurs de crisisafstemming en/of opschaling op Europees niveau wordt beoefend.
Het NCC heeft deze oefening benut om enerzijds de interne procedure met betrekking tot CCA te beoefenen en anderzijds af te stemmen met het ministerie van Buitenlandse Zaken.

Oefening CCAEX09

Het scenario voor deze oefening was vooraf op hoofdlijnen bekend. Het ging om een gijzeling van een high-level delegatie van de EU in een denkbeeldig Afrikaans land. Deze gijzeling ging gepaard met een eis van de groepering aan de EU lidstaten om alle leden van hun groepering die in Europese gevangenissen zitten vrij te laten. Dit scenario vraagt om input van betrokken lidstaten voor het besluit in Brussel en binnen Nederland de betrokkenheid van onder andere de NCTb en het ministerie van Buitenlandse Zaken.

Procedure CCA

De CCA procedure is aanvullend op de reeds bestaande crisis management structuren op Europees en nationaal niveau van de lidstaten. De procedure is in het leven geroepen om een snelle en gecoördineerde respons op Europees niveau mogelijk te maken. De procedure kan worden geactiveerd wanneer qua grootte de crisis meerdere lidstaten treft, dan wel het algemeen belang van de EU raakt. Het kan hierbij zowel om een natuurlijke ramp als een terroristische aanslag gaan.

Uitgangspunt is dat de crisis pijleroverstijgend moet zijn (zowel rampenbestrijding, als bijvoorbeeld consulaire aspecten of terroristische motieven) voorbeelden zijn de Tsunami, en de Londen bombing. Bovendien is het noodzakelijk dat de crisis een politiek gecoördineerde respons op Europees niveau vereist. Met andere woorden, wanneer de crisis enkel operationele actie behoeft, dan is het onwaarschijnlijk dat deze procedure zal worden geactiveerd.

Directeuren Europese collega-instanties brengen bezoek aan het NAVI

Het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) levert als publiekprivate organisatie een structurele bijdrage aan de bescherming van de vitale infrastructuur in Nederland. Het NAVI richt zich op de security van de vitale sectoren en daarbinnen primair op het (helpen) voorkomen van uitval van vitale infrastructuur als gevolg van moedwillig menselijk handelen.

Nationaal Adviescentrum **Vitale Infrastructuur**

Kim Veenendaal, *communicatieadviseur NAVI*

Donderdag 17 september maakte het NAVI werk van zijn internationale platformfunctie door een mini conferentie te beleggen voor directeuren van vergelijkbare organisaties uit Engeland, Duitsland, Spanje en Frankrijk die zich bezighouden met de bescherming van de nationale vitale infrastructuur. Door op deze wijze contact te zoeken en te onderhouden met internationale partijen versterkt het NAVI zijn informatiepositie en kan het NAVI zijn partners beter van dienst zijn: de bescherming van de vitale infrastructuur houdt ten slotte niet op bij de landsgrenzen. Deze eerste bijeenkomst had kennismaking tot doel en om vast te stellen welke mogelijkheden er voor kennisuitwisseling zijn. De aanwezige organisaties gaven een exposé over de, soms sterk uiteenlopende, CIP-aanpak (Critical Infrastructure Protection) in hun landen en welke rol de eigen organisatie daarin heeft. Ook werden good practices gedeeld over het betrekken van private organisaties bij bescherming van de vitale infrastructuur en de ervaringen die daarbij zijn opgedaan.

Alle landen zo bleek, hebben de bescherming van de vitale infrastructuur de laatste jaren aanmerkelijk versterkt en ook een centraal contactpunt gecreëerd. Soms als onderdeel van een ministerie, soms als een zelfstandige organisatie die zich bezighoudt met de bescherming van de vitale infrastructuur. Spanje en Engeland hebben een met NAVI vergelijkbare organisatie, respectievelijk het National Centre for Critical Infrastructure Protection (CNPIC) in Spanje en het Centre for the Protection of National Infrastructure (CPNI) in Engeland. In Frankrijk en Duitsland zijn de taken belegd bij een ministerie.
In Frankrijk is het Secrétariat Général de la Défense Nationale (SGDN) verantwoordelijk voor alle taken die betrekking hebben op de bescherming van de vitale infrastructuur. Duitsland heeft de taken verdeeld over het ministerie van Binnenlandse Zaken (Bundesministerium des Innern, BMI) en het Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK).

Evenals in Nederland blijven de voor de sectoren afzonderlijk verantwoordelijke vakdepartementen ook in de andere landen verantwoordelijk voor (een deel van) de uitvoering van het beleid en de wet en regelgeving. De aanpak verschilt echter.
In Frankrijk wordt de bescherming van de vitale infrastructuur vooral gereguleerd in uitgewerkte regelgeving en voorschriften vanuit de overheid. In Spanje, Engeland en Duitsland wordt de bescherming van de vitale infrastructuur, net als in Nederland, meer geregeld op basis van algemene beleidsnoties, en geschiedt de concrete uitvoering voor zover mogelijk op basis van publiekprivate samenwerking. In Duitsland zijn de provincies (de Länder) autonoom en is de locale overheid verantwoordelijk voor de bescherming van de vitale infrastructuur binnen de ländergrenzen. Op federaal niveau worden voornamelijk richtlijnen uitgewerkt. Doordat zowel Spanje als Engeland in het verleden talrijke voorbeelden van terrorisme kenden, ligt het accent in de strategieën van deze landen op het voorkomen van terroristische aanslagen. Maar ook in deze landen wordt – evenals in Nederland – de bescherming van de vitale infrastructuur tegen moedwillige dreigingen vrij breed en soms zelfs nog iets breder opgevat.

Het overleg tussen het NAVI en zijn partners zal in de toekomst vooral gericht zijn op tactische en praktische onderwerpen van security en infrastructuurbescherming, die gezamenlijk kunnen en moeten worden opgepakt. Het overleg werd door alle partijen als zeer nuttig ervaren en zal in het voorjaar van 2010 worden georganiseerd door Spanje. Voor meer informatie over internationale activiteiten van het NAVI is Marian Kok (adviseur bij het NAVI) via marian.kok@navi-online.nl bereikbaar.

Loco voor de leeuwen
draagt bij aan crisisbeheersing

Nico de Gouw,
projectmanager Crisiscommunicatie
provincie Gelderland

Opnieuw schiet het Nederlands Genootschap van Burgemeesters met *Loco voor de leeuwen* in de crisiscommunicatieroos. Naast het onderhoudende en vooral leerzame zicht op de persoonlijke crisiservaringen van locoburgemeesters benadrukt de bundel interviews de noodzaak voor verantwoordelijke bestuurders om optimaal voorbereid te zijn op mogelijke crisissituaties.

De auteurs Wouter Jong en Roy Johannink hebben tien interviews uitgewerkt met wethouders of oud-wethouders die zelf de leiding hadden bij crises. Daarbij ligt de nadruk in de interviews op de persoonlijke ervaringen, de persoonlijke dilemma's, de mate waarin men voorbereid was en de lessen die men aan andere wethouders wil meegeven. Net als eerder in berichten over ervaringen van burgemeesters in crisissituaties, voert ook bij de wethouders het onverwachte, het gebrek aan voorbereiding, de communicatie richting de bevolking en de persoonlijke impact de boventoon.
Veel wethouders staan verder van de burgemeesterspraktijk af waarin contacten met (crisis)partners als brandweer, politie, Openbaar Ministerie en waterschap voortdurend aan de orde zijn. Als je dan ineens een gemeentelijk beleidsteam moet voorzitten is dat vaak lastig, maar de interviews met de loco's geven aan dat deze 'achterstand' door een authentieke aanpak en opstelling ook wel beperkt kan worden.
De bundel zoomt in op de rol van de locoburgemeester in zowel de voorbereiding (preparatiefase), de alarmeringsfase, de responsfase als in de nazorg. De relatie met de media krijgt ook ruime aandacht.
De geïnterviewden zijn Rinda den Besten als locoburgemeester in Utrecht, Michel Bezuijen in Haarlemmermeer, Henk Brink voorheen Amersfoort, Harry Fellinger in Leek, Jelle Hekman in Amersfoort, Eric Helder in Enschede, Henk Kosmeijer in Tynaarlo, Siebe Kramer indertijd in Moerdijk, Helma Lodders in Zeewolde en Marriët Mittendorff in Eindhoven.

Samenwerking NGB en Wethoudersvereniging

Het NGB heeft voor de totstandkoming van de publicatie nauw samengewerkt met de Wethoudersvereniging. Het illustreert de grote verantwoordelijkheid in de lokale crisisbeheersing van zowel de burgemeester als de wethouder in zijn of haar hoedanigheid van locoburgemeester. Beide bestuurders moeten van elkaar weten dat ze voldoende voorbereid zijn. Zij moeten als tandem kunnen samenwerken en de loco moet de burgemeester naadloos kunnen aanvullen. De lessen die de bundel destilleert kunnen daaraan een bijdrage leveren.

Openhartigheid levert nuttige lessen op

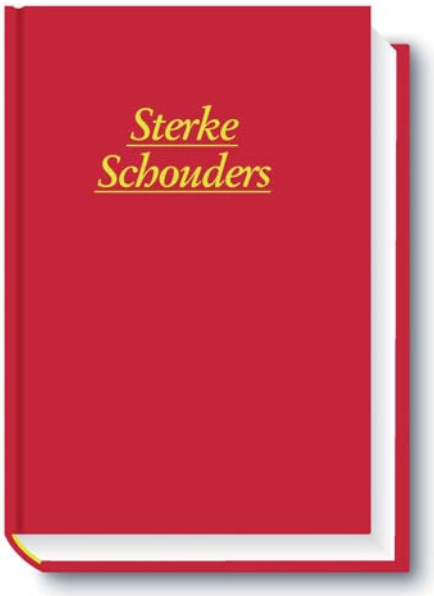
Eigenlijk is de formule van de NGB-interviewbundels eenvoudig en doeltreffend: plaats een serie gesprekken bij elkaar en voeg een aantal algemene lessen en conclusies toe. Dat levert op zich al een nuttig werkstuk op waarmee geïnteresseerde bestuurders hun voordeel kunnen doen. De openhartigheid waarmee de wethouders in de keuken laten kijken, zorgt voor de meerwaarde en persoonlijke herkenning. Iedereen immers die een crisis meemaakt, herkent elementen als eenzaamheid, emoties en daadkracht op momenten die ertoe doen. Een uiterst nuttige publicatie dus, onmisbaar voor gemeentebestuurders. Immers, iedereen kan met een crisis te maken krijgen. Ook al is de wethouder tweede, derde of zelfs vierde locoburgemeester. Om goede nota van te nemen!

"*Loco voor de leeuwen. Crisiservaringen van locoburgemeesters*" is in september door het NGB naar alle burgemeesters en wethouders gestuurd. Na de gemeenteraadsverkiezingen in maart 2010 ontvangen ook de dan nieuwbenoemde wethouders een boekje. De interviews zijn als pdf te downloaden via www.burgemeesters.nl/crisisbeheersing.

Persoonlijke ervaringen geüniformeerde hulpverleners in crisistijd

Michel Dückers,
senior beleidsmedewerker, Impact
Wouter Jong,
coördinator crisisbeheersing, Nederlands Genootschap Burgemeesters

Sterke schouders
in het publieke domein



Impact, het landelijk kennis- en adviescentrum voor psychosociale nazorg na rampen en ingrijpende gebeurtenissen, komt in december met een nieuwe interviewbundel. Na de bundel *Wereld van verschil*, waarin getroffenen en professionals in de crisisbeheersing vanuit twee kanten hun ervaringen met crises belichten, legt Impact in de bundel *Sterke schouders* het vergrootglas op de hulpverlening door geüniformeerden in het publieke domein. De interviewbundel bevat persoonlijke verhalen van ambulancebroeders, brandweerlieden, militairen, politieagenten en reddingswerkers die in hun professionele werk ingrijpende situaties van nabij hebben meegemaakt. Ook komen een meldkamermedewerker, een rechercheur en een urgentiearts aan het woord. Zij vertellen over het werk in een noodsituatie, over de hulpverlening in dringende situaties, over de opvang van collega's en nabestaanden. Daarnaast geven zij een inkijk in de organisaties waar zij deel van uitmaken en de manier waarop zij de media hebben beleefd. Zo vertelt Mayke Aerts over de fotografen die zich in Haarlemmerliede door een politieafscheiding naar het spoor proberen te wringen, waar kort daarvoor een vader met zijn twee kinderen voor de trein is gesprongen. Carlo van der Maar biedt hulp op Koninginnedag en ziet later pas de nietsverhullende foto's die van hem geschoten zijn. Maar Carlo kent ook een andere werkelijkheid. Persfotograaf Paul Groeneveld legde in Apeldoorn zijn camera neer en ging samen met hem over tot reanimatie.

Geüniformeerde hulpverleners vervullen een onmisbare maatschappelijke rol. Sommigen bewegen rondom getroffenen, al dan niet onder het toeziend oog van toeschouwers en verslaggevers met of zonder camera. Anderen werken juist meer achter de schermen, zoals een technisch rechercheur die na een geruchtmakende moord op een basisschool het onderzoek coördineert, terwijl de bloemenzee buiten het schoolgebouw aangroeit.
Ieder maakt eigen inschattingen en afwegingen. Het is de combinatie van die relatief grote beslissingsruimte en de chaotische context van het publieke domein waarin zij verkeren die ertoe bijdraagt dat het werk van de geüniformeerde tot de verbeelding spreekt. Een doorgaans onderbelichte vraag is wat de situaties waarmee zij te maken krijgen met hen persoonlijk doen. Deze bundel met de openhartige verhalen van mensen achter het uniform gaat op die vraag in. Er wordt een beeld geschetst van de praktijk van de geüniformeerde en de complexe relatie waarin zij soms staan met anderen. Niet alleen media en externe onderzoekers, maar ook collega's en dierbaren. Ook is terug te zien hoe zij kampen met onmacht, onbegrip, ongefundeerde kritiek van buitenstaanders en zelfs bedreiging.

De situaties waarin zij verzeild raken, maken weliswaar onderdeel uit van het werk, maar het zijn geenszins vanzelfsprekende situaties. Waar anderen terugdeinzen, treedt de geüniformeerde op. Zoals Xander Beenhakkers die tijdens de Huldigingsrellen van Feyenoord de straat op gaat om collega's in nood te ontzetten. Als hij en zijn collega's merken dat Rotterdamse politie geen grip meer heeft op de relschoppers op de Coolsingel doen zij een stap naar voren. Of het doortastende optreden van Michael Bosch die als medewerker op de alarmcentrale voorkomt dat een vader zijn eigen leven op het spel zet in een vruchteloze poging om zijn zoon te redden in een brand.

Geüniformeerden handelen uit een roeping. Het uiterste wordt soms van hen gevraagd. De samenleving mag deze mannen en vrouwen niet in de kou laten staan. Zij verdienen begrip en erkenning.

De bundel Sterke Schouders in het publieke domein is verkrijgbaar via Impact. Voor meer informatie: http://www.impact-kenniscentrum.nl.

Vanaf volgend jaar komt er een nieuw communicatienetwerk waarmee overheden en vitale organisaties tijdens een ramp of crisis kunnen telefoneren, faxen, e-mailen, data kunnen uitwisselen en zelfs vergaderen met een beeldverbinding. Het nieuwe netwerk blijft beschikbaar als het gewone vaste telefoonverkeer tijdens een ramp uitvalt door overbelasting of stroomuitval. Zelfs het gebruik van mobiele telefoons is mogelijk wanneer het gewone gsm-verkeer door overbelasting uitvalt. Het netwerk vervangt het verouderde Nationaal Noodnet, dat sinds 1991 in de lucht is maar alleen telefoon en fax ondersteunt.

Nieuw noodcommunicatienetwerk voor bestuurlijk Nederland en vitale organisaties bij ramp of crisis

Het contract voor het nieuwe noodcommunicatienetwerk (officieel "NoodCommunicatieVoorziening NCV") is medio november namens minister Ter Horst getekend door Dick Schoof, directeur-generaal Veiligheid bij BZK, en door Eelco Blok, lid Raad van Bestuur van KPN, leverancier van het nieuwe netwerk.

Het gaat om een meerjarige raam-overeenkomst, waarin KPN de diensten van het nieuwe noodnet aan de gebruikers aanbiedt. De gebruikers kunnen zelf kiezen van welke diensten zij gebruik willen maken: alleen bellen en faxen of ook berichten-verkeer (e-mail), mobiele telefonie en 'beeldbellen' met een videoverbinding. Op termijn zullen nog meer diensten beschikbaar komen.

Op dit moment zijn er zo'n 5500 aansluitingen op het Nationaal Noodnet. Een groot deel hiervan bevindt zich in de sectoren openbaar bestuur en veiligheid, zoals het Nationaal Crisiscentrum, coördinatiecentra van provincies, gemeentehuizen, regionale meldkamers van politie en veiligheidsregio's en ziekenhuizen. De andere gebruikers zijn organisaties en instanties die behoren tot de vitale sectoren en die in crisisomstandig-heden een specifieke taak hebben. Voorbeelden hiervan zijn o.a. energie- en waterbedrijven, waterschappen, omroepen, de spoorwegen, meldkamers voor het openbaar vervoer en belangrijke ict- en telecomknooppunten.

Het huidige Noodnet heeft aparte telefoon- en faxtoestellen. In het nieuwe netwerk wordt het mogelijk via gewone telefoons, faxen en computers toegang te krijgen. Dat is gemakkelijker voor de gebruikers en biedt ook nieuwe mogelijkheden.

Uitgaande van het huidige aantal van 5500 abonnees zijn de kosten voor de basisdienst-verlening voor de gebruiker gelijk aan het huidige Noodnet. Naar schatting komt de totale waarde van het afgesloten raam-contract uit op ruim 6,5 miljoen euro per jaar.

Het noodnet is een vast telefoonnetwerk voor bestuurders en vitale organisaties; niet te verwarren met C2000, het netwerk voor mobiele communicatie via portofoons en mobilofoons voor politie, brandweer, ambulances en marechaussee.

(Bron: Persbericht ministerie van BZK, 18 november 2009)

Colofon

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

Redactie
Redactiecommissie: Henk Geveke, Marije Breedveld, Nelly Ghaoui, Lodewijk van Wendel de Joode en Geert Wismans (samenstelling en eindredactie)
Redactiesecretariaat: Nalini Bihari (070-426 53 00)

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

Aan dit nummer werkten mee:
Ben Ale, Ana Lidia Aneas Moyano, Fatma Aytekin, Melle Bakker, Ank Bijleveld-Schouten, Arjen Boin, Marc Bökkerink, Jan Willem van Borselen, Anja van den Bosch-Overduin, Ernst Brainich, Ella Broos, Marian Byvanck, Maike Delfgaauw, Michel Dückers, Menno van Duin, Roos van Erp-Bruinsma, Mark Frequin, Sabine Geerdes, Nico de Gouw, André Griffioen, Jos Groot, Floris de Haan, Ira Helsloot, Peter Hondebrink, Bart Jacobs, Rob Jastrzebski, Wouter Jong, Frank Kalshoven, Floor Keijsers, Jos Klaren, Jenny Kossen, Douwe Leguit, Carlo Luijten, Nils Ligthart, Caroline Linssen, Eric Luiijf, Erik Moonen, Erwin Muller, Leo Nieuwenhuizen, Ragna Opten, Tom Orton, Hans Oude Alink, Dick Schoof, Astrid Scholtens, N. Schuurhuizen, Peter Sloot, Erwin Seydel, Ton Slewe, Pim Takkenberg, C. Timmer, Marieke Timmermann, Nora Timmermans, M. Tuinder, Kim Veenendaal, Pauline Veldhuis-Beem, Hans van der Vlist, Hans de Vries, Peter Werkhoven, Rob de Wijk, Geert Wismans, Anja van Zantvoort, Annemarie Zielstra

Fotografie
112 fotografie, ANP, FEMA, GOVCERT.NL, Hollandse Hoogte, Bob van der Kamp, Eric Planquart, Gerhard van Roon, Arthur Wijnen

Illustraties
De Argumentenfabriek, Burobraak, ENISA, GOVCERT.NL

Cartoons
Arend van Dam

Vormgeving
Grafisch Buro van Erkelens, Den Haag

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

Druk
OBT bv, Den Haag

ISSN 1875-7561

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

Het magazine is te downloaden via www.minbzk.nl/veiligheid/crisisbeheersing/magazine.

Vier vragen aan:

Ank Bijleveld-Schouten, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

U houdt zich bezig met de E-overheid en met dienstverlening. Wat hebben die te maken met veiligheid en crisisbeheersing?
"Als de burgers de overheid niet vertrouwen met hun informatie, dan zal er nauwelijks sprake kunnen zijn van e-overheid. En als door een grote stroomuitval de digitale wereld ontoegankelijk wordt, komt een belangrijk deel van het werk van de overheid tot stilstand en kunnen burgers en overheid elkaar niet meer bereiken. Met andere woorden e-overheid en dienstverlening hebben alles te maken met veiligheid en crisisbeheersing."

Wat doet u voor burgers en bedrijven?
"We werken aan het verbeteren van de dienstverlening aan burgers en bedrijven door administratieve lasten- en regeldruk-vermindering en door de inzet van slimme en betrouwbare ICT. Via internet kunnen burgers en bedrijven steeds bij de overheid terecht voor bijvoorbeeld het raadplegen van de eigen persoonsgegevens, het aanvragen van voorzieningen voor chronische zieken of de belastingaangifte via een elektronisch formulier.
Het is daarbij cruciaal dat burgers en bedrijven de overheid volledig kunnen vertrouwen voor een veilige en beschermde verwerking van gegevens en transacties. We doen dit onder andere door EPD-Digid voor een veilige toegang, door PKI-overheid voor veilige gegevensuitwisseling en door alertering voor virussen en criminele acties op het internet door GOVCERT.NL en de Waarschuwingsdienst. Burgers, die zich zorgen maken over ID-fraude of vermoeden dat zij slachtoffer zijn geworden van ID-fraude, kunnen zich wenden tot het Meldpunt Identiteitsfraude dat er is om individuele burgers te helpen."

Wat merkt de professional in het veiligheids-domein van dit alles?
"Het gebruik van BSN en EPD-Digid versterkt het betrouwbaar en slagvaardig handelen van de professional. Met DigiD kan de transactie-dienstverlening aan burgers laagdrempeliger en het handelen van de overheid transparanter worden gemaakt. Ik zou dan ook graag zien dat DigiD in de Veiligheidssector nog meer wordt toegepast. Goede voorbeelden zijn de aangiftevolgservice van mijnpolitiebureau.nl en de online flitsfoto's van de eigen verkeersovertreding.
Wat betreft de juiste gegevens moet de veiligheidssector gebruik maken van de basisregisters zoals de Gemeentelijke Basis Administratie (basisregister personen), het Nieuw Handelsregister, het Basisregister voor Adressen en Gebouwen, het Kentekenregister en het Basisregister Kadaster en Topografie. Het gebruik van de basisregisters wordt bij wet geregeld. De basisregistraties dienen te worden geïntegreerd in de eigen werkprocessen.
Het grote voordeel is dat de professional in het veiligheidsdomein beschikt over actuele en betrouwbare gegevens over personen, bedrijven, voertuigen, gebouwen, percelen, topografie, etc. Het slagvaardig en adequaat handelen wordt hiermee sterk verbeterd. Verder worden dubbele gegevensopslag en dus ook dubbele kosten voorkomen.
Ten slotte zorgt het stelsel van basis-registraties ervoor dat eventuele fouten kunnen worden teruggemeld en na onderzoek kunnen worden gecorrigeerd."

Wat zijn uw ambities voor de informatie-beveiling?
"Ik weet dat informatiebeveiliging om voortdurende aandacht vraagt. Daarom zijn er maatregelen nodig om de informatie-beveiliging voortdurend op peil te houden. Zoals ik tijdens het GOVCERT.NL symposium Initiating Change op 6 en 7 oktober jl. heb gezegd wil ik een zichtbare kwaliteits-verbetering in de informatiebeveiliging. Ik wil hiervoor ook de aandacht vragen van de Chief Information Officers van de departementen. Tevens moeten er waar nodig hoogwaardige 'security' organisaties worden ingericht, de periodieke auditing van de ICT-veiligheid worden verscherpt, de adviezen van GOVCERT.NL worden opgevolgd, het versiebeheer en patch-management strikt worden uitgevoerd, etc. Daarnaast wil ik nagaan of het mogelijk is om een meldplicht voor ICT-incidenten bij de rijksoverheid in te stellen, dit naar analogie van de meldplicht van verlies van persoons-gegevens door bedrijven."